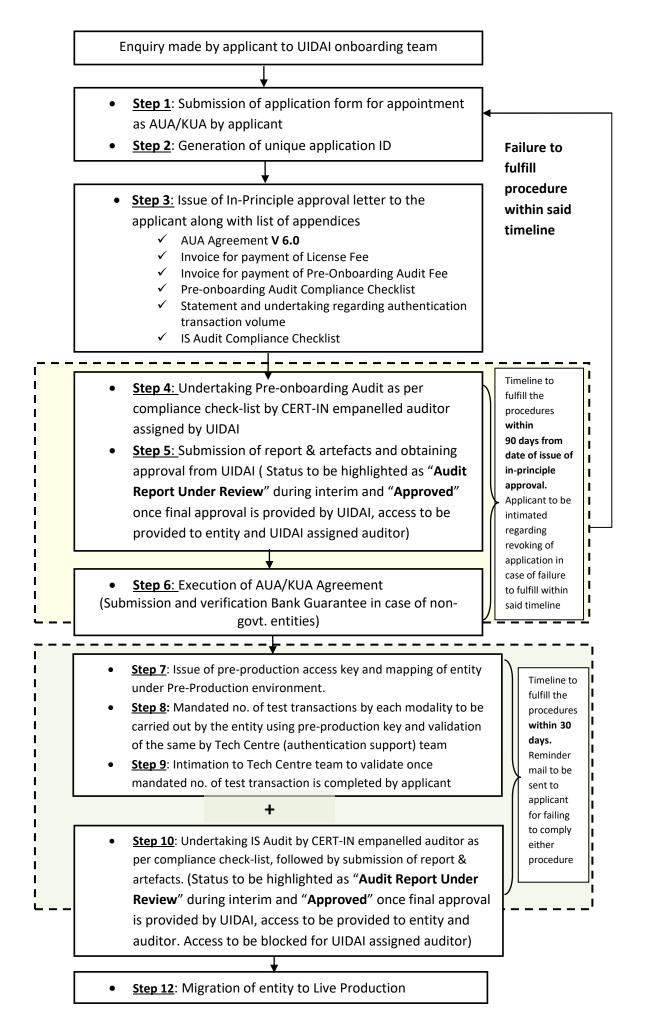
A process flow diagram elucidating the entire onboarding process of AUA/KUA is as shown below:-



Application form for

Appointment as Authentication User Agency (AUA) and e-KYC User Agency (KUA)

To:

The Chief Executive Officer, Unique Identification Authority of India [Attention: Deputy Director (Authentication-II), UIDAI] UIDAI Head Office, Bangla Sahib Road

1. D	1. Details of the applicantMinistry, Department, secretariat, office or agency of the Central					
Gov	vernment, a State Government or the Go	wernment/Administration of a Union territory, or other				
enti	ty:					
(a)	Name of the applicant ¹					
(b)	Registration/ Incorporation No. ²					
	(Please attach copy of the document, if					
	applicable)					
(c)	License No. ³					
	(Please attach copy of the document, if					
	applicable)					
(1)	D 1 (C 11					
(d)	Registered office address					
(e)	Correspondence address					
	{If other than address mentioned					
	against (d)}					
(f)	GSTN registration number of the					
	applicant, as per Form GST REG-06					
	(Please attach copy of the document, if					
	applicable)					
(g)	Tax Deduction and Collection Account					
	Number(TAN) of the applicant					
	(Please attach copy of the document, if					

2 Copy of Certificate of incorporation/registration to be attached in case of "other than Govt. entities"

¹Name of the applicant Ministry, Department, secretariat, office or agency of the Central Government or the Government of State or Union territory, or other applicant entity

³ Copy of Certificate of Registration/License from the concerned Regulator issued from RBI, SEBI, IRDAI and PFRDA

	applicable)	
(h)	Type of Aadhaar Authentication facility; Corresponding category of requesting entity (<i>Tick as applicable</i>)	 Yes/No Authentication facility; AUA Yes/No Authentication facility and e-KYC Authentication facility; AUA and KUA
(i)	Board resolution/minutes (or other valid letter/instrument of authorisation)citing approval for submitting the application form, signing Authentication User Agency Agreement and doing other acts in relation to the same (<i>Please attach certified copy of the</i> <i>document</i>)	
(j)	The provision of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 under which authentication is required/permitted {If such provision is section 7 or section 4(4)(b)(ii) or section 4(4)(b)(i) read with the Prevention of Money- laundering Act, 2002, please attach copy of the relevant notification published in the Official Gazette}	 Section 7 Section 4(4)(b)(i), read with the Prevention of Money- laundering Act, 2002 Section 4(4)(b)(i), read with relevant Central Act other than the Prevention of Money-laundering Act, 2002 Section 4(4)(b)(ii) Section 4(7)
(k)	Category of the applicant Ministry/Department/ secretariat/office/agency/entity	AMinistry, Department, secretariat, office, or agency of the Central Government, which has required, in terms of the provisions of section 7 of the Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of India
		☐ A Ministry, Department, secretariat, office or agency of the Government of4, which requires, in terms of the provisions of section 7 of Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of State
		An entity permitted under sub-clause (i) of clause (b)

⁴ Name of the concerned State, or the concerned Union territory with Legislature

	of sub-section (4) of section 4 of the Act to offer authentication services under ⁵ of ⁶ .
	☐ An entity permitted under sub-clause (i) of clause (b) of sub-section (4) of section 4 of the Act to offer authentication services under section 11A of the Prevention of Money-laundering Act, 2002, by virtue of being a reporting entity under the said Act as a ⁷ , in terms of ⁸ of sub-section (1) of section 2 of the said Act.
	An entity that has been allowed/authorised under sub- clause (ii) of clause (b) of sub-section (4) of section 4 of the Act, vide Ministry of Electronics and Information Technology's letter no. ⁹ , dated ¹⁰ .
	An entity that is required, in terms of the provisions of sub-section (7) of section 4 of the Act, to perform mandatory authentication by of^{11}.
2. Contact details:	
(a) Management Point of Contact (MPOC)	Person authorised on the basis of Board resolution/minutes (or other valid letter/instrument of authorisation)
Name	
Full designation	

⁵ Reference of the relevant provision (section, sub-section, clause etc.) of the relevant Act of Parliament, other than the Prevention of Money-laundering Act, 2002 ("PML Act")

⁶ Name of the relevant Act of Parliament, other than the PML Act

⁷ banking company, or financial institution, or intermediary, or a person carrying on activities for playing games of chance for cash or kind, or Inspector-General of Registration appointed under section 3 of the Registration Act, 1908, or Central-Government-notified real estate agent, or Central-Government-notified dealer in precious metals, precious stones and other high value goods, or Central-Government-notified person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, or Central-Government-notified person carrying on such other activities (whichever is applicable)

⁸ clause (wa), or sub-clause (i) of clause (sa), or sub-clause (ii) of clause (sa), or sub-clause (iii) of clause (sa), or sub-clause (iv) of clause (sa), or sub-clause (v) of clause (sa), or sub-clause (sa), or

⁹ Number of the letter so allowing/authorising

¹⁰ Date of the letter so allowing/authorising

¹¹ the provision (section, sub-section, clause etc.) of the Act made by Parliament, other than the Aadhaar Act

Official email address								
Mobile number								
Alternate office/telephone								
number								
(b) Technical Point of	CXO/ Head of the functional vertical, who	Other 1	key personnel (if any)					
Contact (TPOC)	reports to the chief executive or governing							
	body of the applicant Ministry/							
	Department/secretariat/office/agency/entity							
Name								
Ivanie								
Full designation								
Official email address								
Mobile number								
widdle number								
Alternate office telephone								
number								
(c) AUA/KUA	DC (Data Centre)	DR (D	ata Recovery Centre)					
infrastructure details		Dir (D						
MPOC/TPOC Name								
Email address								
Telephone/Mobile No.								
Address								
District								
Stata								
State								
PIN Code								
(d) Contact details for grievance redressal:								
(i) Website URL								
(ii) Email address								

(iii) Helpdesk	
number	
3. Details of Authentication	n Service Agency (ASA)
(a) Name(s) of ASA (In case of multiple ASAs, please provide their names)	1.
 (b) Declaration by the ASA(s) agreeing to provide its/their secure network connectivity and related services for the performance of authentication (Please attach letter) 	
of ASA in original)	
4. Authentication requiren	ients
(a) Territorial extent for use of Authentication facility	 Whole of India Name of State(s) and Union Territory(s):
 (b) Whether Authentication will be used to establish identity for carrying out financial transaction 	Yes No
(c) Device form factor (select one or more option)	Discrete Biometric Device Integrated Biometric Device
	Laptop/Desktop
(d) Whether Authentication will be operator-assisted or by the user himself/herself (selectone or more option)	Operator-assisted use Self-use

(e)	Mode of Authentication	Demographic	DTP
	(selectone or more		
	option)	□ Fingerprint	Iris
		Face	
(f)	Connectivity supported	U VPN	eased line
	between AUA/KUA and ASA		
	(selectone or more		
	option)	Other; Please specify:	
(g)	Confirmation that the	Yes No	
	applicant has perused		
	and understood		
	UIDAI's Information Security Policy –		
	External Ecosystem –		
	Authentication User		
	Agency/ KYC User		
	Agency v6.0		
	(Copy of the said policy document, after		
	affixing the signatures		
	of the authorised		
	signatory, to be		
	attached)		
(h)	Confirmation that the	□ Yes □ No	
	applicant has perused and understood		
	UIDAI's Model		
	Privacy Policy for		
	Protecting Personal		
	data of Aadhaar		
	Number Holders by Requesting Entities		
	(Copy of the said		
	policy document, after		
	affixing the signatures		
	of the authorised		
	signatory, to be attached)		
	······································		

Gole Market, New Delhi – 110 001

Declarationsand Undertakings:

It is hereby declared that the information furnished in this application form is true and correct to the best of its knowledge and that no material particulars or information have been concealed or withheld, and that the

of

(name

undertakes-

(a) to abide by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") and the regulations made thereunder;

applicant Ministry/Department/secretariat/office/agency/entity) hereby

- (b) to facilitate, on receipt of in-principle approval from UIDAI, audit as per UIDAI "Compliance Checklist for Onboarding the Requesting Entity" and submit all compliance related documents attached as annexures before signing the AUA/KUA Agreement;
- (c) to fulfil all requirements with respect to use of the Aadhaar Authentication facility as per the Aadhaar (Authentication and Offline Verification) Regulations, 2021;
- (d) to set up and maintain within the territory of India, at all times, requisite infrastructure (including, but not limited to, servers, databases etc.) for the use of Aadhaar Authentication facilities, capable of handling a minimum of one lakh Authentication transactions per month;
- (e) to carry out appropriate due diligence before engaging any sub-contractor, business correspondent or field operator for performing any functions in relation to the use of Aadhaar Authentication facilities, including onboarding of user/beneficiary/customer, Authentication application development, etc.;
- (f) to store Aadhaar numbers, if authorised so to do, only in the Aadhaar Data Vault, in accordance with such policies, procedures, standards and technical specifications as UIDAI may specify from time to time;
- (g) to ensure the carrying out of audit of its own operations and systems and those of its Sub-AUAs and Sub-KUAs, if any, as required under the Aadhaar Act, the regulations made thereunder and the AUA Agreement;
- (h) to not share or disclose e-KYC data that may be received on use of e-KYC Authentication facility, except in accordance with the provisions of the Aadhaar Act and the regulations made thereunder; and
- (i) to inform UIDAI forthwith of any change in the name, address and other particulars of the applicant and contact persons as furnished in this application form.

(Signature with stamp/seal of authorised signatory)

Name: _____

Full designation: _____

Date: _____

Place: _____

Compliance checklist for verification of information furnished by applicant for appointment as AUA/KUA

Version 1.0 [issued in March 2024]

Important note: Wherever a control description requires AUA/KUA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablements are in place to secure compliance with the same on an ongoing basis.

Control no.	Short title	Control description	Control mapping	Compliance status (Compliant / Non-compliant / Not applicable)	Auditor's observation	Comments of AUA/KUA management
A.	Information	security governance		r	r	
1.	Security	AUA/KUA should				
	organisation	ensure that it has a	Information			
	and CISO	designated Chief	Security Policy			
	function	Information	— UIDAI			
		Security Officer	External			
		(CISO) function	Ecosystem —			
		that oversees	Section 2.3(1)			
		information				
		security				
		governance and				
		compliances. The				
		CISO should have				
		independent				
		reporting to its				
		Board or other				
		governing body or				
		chief executive.				
2.	Appointmen	AUA/KUA should	UIDAI			
	t of	appoint a	Information			
	management	Management	Security Policy—			
	and	Single Point of	UIDAI External			
	technical	Contact (MPOC)	Ecosystem —			
	single point	and Technical	AUA KUA —			
	of contact	Single Point of	Section 2.3			
		Contact (TPOC)				
		that should oversee				
		the management of				
		the authentication				
		application and				
		Aadhaar related				

		activities.			
		uoti vititos.			
		MPOC/TPOC			
		should ensure			
		consistent			
		communication			
		with UIDAI on			
		Aadhaar related			
		requirements and			
		compliances.			
		1			
		Any change in			
		MPOC/TPOC			
		should be			
		communicated to			
		UIDAI in a timely			
		manner.			
3.	Information	AUA/KUA should	UIDAI		
	security	have an	Information		
	policy and	information	Security Policy		
	procedure	security policy and	—UIDAI		
		information	External		
		security	Ecosystem —		
		procedures in	AUA KUA —		
		accordance with	Section 2.9		
		industry leading			
		standards, such as			
		ISO27001 (ISMS),			
		NIST Cyber			
		Security			
		Framework, CSA			
		Framework and			
		ISO27701 (PIMS).			
		The entity's			
		information			
		security policy			
		should also address			
		the security aspects			
		of Aadhaar, as			
		provided under the			
		Aadhaar Act,			
		regulations and			
		specifications.			

4.	Aadhaar	AUA/KUA should	UIDAI		
4.					
		ensure that the	Information		
		authentication	Security Policy		
	design	application design	—UIDAI		
		architecture is	External		
		documented and	Ecosystem —		
		validated by	Section 2.3(5)		
		UIDAI			
		Technology Centre			
		and covers			
		Aadhaar security			
		requirements.			
5.	Aadhaar	AUA/KUA should	UIDAI		
5.		ensure that the	Information		
		Aadhaar data flow	Security Policy		
	design	is properly	— UIDAI		
	design	documented for its	External		
		AUA/KUA	Ecosystem —		
		applications and	Section 2.3(6)		
		those of its Sub-			
		AUAs and Sub-			
		KUAs.			
6.	Risk	AUA/KUA should			
	assessment	implement process	Information		
		and procedure to	Security Policy		
		perform periodic	— UIDAI		
		(atleast annual)	External		
		information	Ecosystem —		
		security risk	Section 2.3(13)		
		assessment of its			
		ICT infrastructure			
		supporting the			
		authentication			
		application.			
		Further, entity			
		should also			
		perform risk			
		assessment of its			
		third party			
		suppliers / vendors			
		having access to			
		the Aadhaar			
		application and the			
		data of Aadhaar			
		number holders.			

7.	Third party information security policy	Security risks should be documented and reviewed periodically by Security Officers / CISO / those incharge of the security governance of the AUA/KUA and its Sub-AUAs and Sub-KUAs. AUA/KUA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (<i>e.g.</i> , third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud	Information Security Policy — UIDAI		
		service providers etc.) are obligated			
В.	Compliance	to adhere to. requirement			
8.	IPR	The AUA/KUA	Authentication		
	provisionsco ntained in UIDAI's Aadhaar User AgencyAgre ement (latest	compliance with the intellectual property provisions	User Agency Agreement version 6.0 — Section 3		
	version)	User Agency			

		Agreement (latest				
		version).				
9.	Annual information security audit by CERT-In- empanelled auditor	AUA/KUA should ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with UIDAI's standards and specifications. The audit report should be shared with UIDAI. If any non- compliance is found as a result of the audit, AUA/KUAshould — (a) determine the causes of the non- compliance; (b) evaluate the need for actions to avoid recurrence of the same; (c) determine and enforce the implementati on of corrective and preventive	•	The Aadhaar (Authenticatio n and Offline Verification) Regulations, 2021 — Chapter III — Clause (h) of sub-regulation (1) of regulation 14 The Aadhaar (Data Security) Regulations, 2016 UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13		
		actions; and				

			1		
		(d) review the			
		corrective			
		actions taken.			
		The summer 1 and 14			
		The annual audit			
		should cover all			
		security controls			
		applicable under			
		the Aadhaar (Data			
		Security)			
		Regulations, 2016.			
10.	Onboarding	AUA/KUA should	The Aadhaar		
	of ASA	ensure that UIDAI	(Authentication		
		is informed of the	and Offline		
		ASAs with whom	Verification)		
		it has entered into	Regulations,		
		agreementto	2021 — Chapter		
		provide necessary	III —Sub-clause		
		infrastructure for	(g) of sub-		
		ensuring secure	regulation (1) of		
		network	regulation 14		
		connectivity and	0		
		related services to			
		it to enable			
		performance of			
		authentication			
		using the			
		Authentication			
		facilities provided			
		by UIDAI.			
C.	Data privacy				
11.	Data Data	AUA/KUA should	• UIDAI		
11.	protection	establish a data	• OIDAI Information		
	policy	protection policy	Security		
	poncy		5		
		addressing, <i>inter</i>	Policy —		
		<i>alia</i> , data protection			
		related aspects	External		
		under—	Ecosystem —		
		(a) the Aadhaar	AUA/KUA —		
		Act, the	Section		
		regulations	2.14(2)		
		made	• The IT Act		
		thereunder	• Till the		
		and the	coming into		
		standards and	force of the		
		specifications	DPDP Act, the		
		issued by	SPDI Rules		

	1 1		
UIDAI from	and, on and		
time to time;	from the date		
(b) the	of coming into		
Information	force of		
Technology	clauses (a) and		
Act, 2000	(c) of sub-		
("IT Act");	section (2) of		
and	section 44 of		
(c) till the coming	the DPDP Act,		
into force of	the said Act		
the Digital	and the rules		
Personal Data	made		
Protection	thereunder ¹²		
Act, 2023			
("DPDP			
Act"), the			
Information			
Technology			
(Reasonable			
Security			
Practices and			
Procedures			
and Sensitive			
Personal Data			
or			
Information)			
Rules, 2011			
("SPDI			
Rules") and,			
on and from			
the date of			
coming into			
force of the			
DPDP Act,			
the said Act			
and the rules			
made			
thereunder.			
Such policy should			
be published on			
the website of			
AUA/KUA and the			
URL for the same			
should be			

¹²See clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, read with clause (ob) of sub-section (2) of section 87 and section 43A of the IT Act

		mentioned.			
12.	Consent of	The AUA/KUA	The Aadhaar		
	Aadhaar	should obtain	(Authentication		
	number	consent of the	and Offline		
	holder	Aadhaar number	Verification)		
		holder or, in case	Regulations,		
		of a child, the	2021 — Chapter		
		consent of the	II — Regulation 6		
		parent or legal			
		guardian of such			
		child, before			
		collecting their			
		identity			
		information for the			
		purposes of			
		authentication. The			
		consent should be			
		obtained			
		preferably in			
		electronic form.			
13.	Information	At the time of	The Aadhaar		
	to Aadhaar	authentication,	(Authentication		
	number	before obtaining	and Offline		
	holder on	consent,	Verification)		
		AUA/KUA should	U ,		
		inform the	2021 — Chapter		
	that will be	Aadhaar number	II —Clause (a) of		
	-	holder or, in case	sub-regulation (1)		
	performance		of regulation 5		
	of	parent or legal			
	authenticatio	guardian of such			
	n	child, regarding the			
		nature of			
		information that			
		will be shared by			
		UIDAI upon			
		performance of			
		authentication.			
14.	Information	At the time of	The Aadhaar		
	to Aadhaar	authentication,	(Authentication		
	number	before obtaining	and Offline		
	holder on	consent,	Verification)		
	use of	AUA/KUA should	Regulations,		
	information	inform the	2021 — Chapter		

	magnitud	A adhaan numban	$\mathbf{H} = \mathbf{C}$ laws (b) of		[]
	received	Aadhaar number	II —Clause (b) of		
	during	holder or, in case	sub-regulation (1)		
	authenticatio	,	of regulation 5		
	n	consent of the			
		parent or legal			
		guardian of such			
		child, of the uses			
		to which the			
		information			
		received during			
		authentication may			
		be put to by it.			
15.	Alternative	At the time of	The Aadhaar		
101	mechanisms	authentication,	(Authentication		
	for	before obtaining	and Offline		
	submission	consent,	Verification)		
		AUA/KUA should			
	of identity		Regulations,		
	information	inform the	2021 — Chapter		
		Aadhaar number	II —Clause (c) of		
		holder or, in case	sub-regulation (1)		
		of a child, the	of regulation 5		
		parent or legal			
		guardian of such			
		child, of the			
		alternatives to			
		submission of			
		identity			
		information.			
16.	Consent	The AUA/KUA	• The Aadhaar		
	communicat	should ensure that	(Authenticatio		
	ion in local	the consent	n and Offline		
	language	information is	Verification)		
		communicated in	Regulations,		
		local language.	2021 —		
			Chapter II —		
		The AUA/KUA	Sub-regulation		
		should also ensure	(2) of		
		that, on and from	regulation 5		
		the date of coming	 On and from 		
		into force of sub-	the date of		
		section (3) of			
		section 5 of the	coming into force of sub-		
		DPDP Act, the			
		Aadhaar number	section (3) of		
			section 5 and		
		holder has the	sub-section (3)		
		option to access	of section 6 of		
		the contents of the	the DPDP Act,		

		notice referred to	the said Act —		
		in sub-sections (1)	Sub-section		
		and (2) of the said	(3) of section		
		sectionand the	5 and sub-		
		request for consent	section (3) of		
		referred to in sub-	section 6		
		section (3) of			
		section 6in English			
		or any language			
		specified in the			
		Eighth Schedule to			
		the Constitution.			
17.	Communicat	The AUA/KUA	UIDAI		
	ion of	should make	Information		
	consent	provisions for	Security Policy		
	related	communication of	— UIDAI		
	information	consent related	External		
	to persons	information to	Ecosystem —		
	with		AUA/KUA —		
		persons with	Section 2.14		
		visual/hearing	Section 2.14		
	g disability	disability in an			
		appropriate			
		manner.			
18.	Explicit	AUA/KUA should	_		
	consent; no	ensure that the	Information		
	umbrella	consent taken from	Security		
	consent	the Aadhaar	Policy —		
		number holder	UIDAI		
		should in	External		
		accordance with	Ecosystem —		
		the provisions of	AUA/KUA —		
		the Aadhaar Act,	Section 2.9		
		2016 and the	• On and from		
		regulations made	the date of		
		thereunder;no	coming into		
		umbrella consent	force of sub-		
		should be taken for	section (1) of		
		sharing e-KYC or	section 5 and		
		Aadhaar number of			
		the Aadhaar	sub-section (1)		
		number holders	of section 6 of		
			the DPDP Act,		
		with other entities.	the said Act —		
			Sub-section		
		The AUA/KUA	(1) of section		
		should also ensure	5 and sub-		
		that,on and from the date of coming	section (1) of		

		into force of sub-				
		section (1)of				
		section 5 and sub-				
		section (1) of				
		section 6 of the				
		DPDP Act, the				
		consent taken from				
		the Aadhaar				
		number holder is				
		in accordance with				
		the applicable				
		provisions of				
		sections 5 and 6 of				
		the said Act.				
D.	Asset manag	ement	I		I	<u> </u>
19.	Biometric	AUA/KUA should	•	The Aadhaar		
	device	capture the		(Authenticatio		
	management	-		n and Offline		
	management	information of the		Verification)		
		Aadhaar number		Regulations,		
		holder using		2021 —		
		certified and		Chapter II —		
		registered		Clause(a) of		
		biometric devices				
				sub-regulation		
		as per standards		(1) of		
		specified by		regulation 7,		
		UIDAI from time		sub-regulation		
		to time.		(1) of		
				regulation 8		
				and clause (d)		
				of sub-		
				regulation (1)		
				of regulation		
				14		
			•	UIDAI		
				Information		
				Security		
				Policy —		
				UIDAI		
				External		
				Ecosystem —		
				AUA/KUA —		
				Section 2.4		

20.	End-point	AUA/KUA should	Advisory		
20.	security	ensure that	regarding		
	security	biometric	strengthening of		
		deploying devices	Biometric		
		are connected with	authentication		
		end-point systems	security		
		that have the latest	[AdvisoryF. no.		
		operating system	13043/2/2021-		
		(OS) specifications			
		(as of March 2024,	dated 31.5.2022]		
		at least Windows			
		10 and above and			
		Android OS 10			
		and above), and			
		that systems based			
		on an OS that is			
		end-of-life or end-			
		of-support are not			
		deployed or used.			
21.	Security	AUA/KUA should	UIDAI		
	hardening of	ensure all the end-	Information		
	assets	point devices and	Security Policy		
		assets are used	— UIDAI		
		only after	External		
		hardening to	Ecosystem —		
		reduce/eliminate	AUA KUA —		
		the attack vector	Section 2.4		
		and condense the			
		system attack			
		surface.			
22.	Maintenance				
	of software	ensure that it uses	Information		
	inventory	only licensed software for	Security Policy — UIDAI		
		Aadhaar	External		
		authentication			
		related	Ecosystem — AUA KUA —		
		infrastructure	Section 2.13		
		environment.	Section 2.15		
		Record of all			
		software licenses			
		should be kept and			
		updated regularly.			
		updated regularly.			

23. Asset AUA/KUA should UIDAI	
disposal define a procedure Information	
procedure for disposal of the Security Policy	
information assets —UIDAI	
being used for External	
authentication Ecosystem —	
operations. AUA KUA —	
Information Section 2.4	
systems and	
documents	
containing	
Aadhaar related	
information should	
be disposed of	
securely.	
E. Human resource security	
24. Background AUA/KUA should UIDAI	
verification conduct a Information	
and signing background check Security Policy	
of and sign a —UIDAI	
confidentiali confidentiality External	
ty agreement/ non- Ecosystem —	
disclosure AUA KUA —	
agreement (NDA) Section 2.3	
with all	
personnel/agency	
handling Aadhaar	
related	
information.	
Access to	
authentication	
infrastructure	
should not be	
granted before	
signing NDA and	
completion of	
background	
verification(BGV)	
for personnel.	
25. Background AUA/KUAshould UIDAI	
verification take an Information	
and signing undertaking from Security Policy	
of business —UIDAI	
confidentiali correspondents External	
ty agreement (BCs) and similar Ecosystem —	
with third- entities, Sub- AUA KUA —	
party AUAs/Sub-KUAs Section 2.3	

	contractors	and other third			
		party contractors			
		regarding NDAs			
		and BGVs			
		conducted			
		successfully for			
		their personnel			
		handling Aadhaar			
 		related data.			
26.	Training and		UIDAI		
	awareness	ensure that MPOC,			
		TPOC and their	Security Policy		
		supporting teams	— UIDAI		
		that manage and	External		
		maintain the	Ecosystem —		
		authentication	Section 2.3(7)		
		application and its			
		underlying			
		infrastructure, are			
		aware of Aadhaar			
		security			
		requirements.			
27.	Operator	AUA/KUA should	The Aadhaar		
	qualification	ensure that the	(Authentication		
	1	operator employed	and Offline		
		for performing	Verification)		
		authentication	Regulations,		
		functions and	2021 — Chapter		
		maintaining	III —Clause (f)		
		necessary systems,	of sub-regulation		
		infrastructure and	(1) of regulation		
		process, possess	14		
		requisite	17		
		qualification for			
		-			
		undertaking such work.			
 20	Doriadia	WORK. AUA/KUA should			
28.	Periodic		UIDAI		
	information	impart information			
	security and	security and data	Security Policy		
	privacy	privacy trainings to			
	trainings	all its personnel as	External		
	related to	well as those of	Ecosystem —		
	Aadhaar	any BCs, Sub-	AUA KUA —		
	authenticatio		Section 2.3		
	n operations	and similar			
		entities, in relation			
		to the use of			

F.	Incident management		
	trainings imparted.		
	record of such		
	also maintain a		
	AUA/KUA should		
	time to time.		
	by UIDAI from		
	notices etc. issued		
	and circulars,		
	made thereunder		
	and the regulations		
	Aadhaar Act, 2016		
	Authentication,		
	Security Policy for		
	Information		
	the UIDAI		
	guidelines, as per		
	and data privacy		
	relevant security		
	the same cover all		
	ecosystem and that		
	the authentication		
	roles involved in		
	various functional		
	are imparted for		
	specialised training		
	specific and		
	further ensure that		
	AUA/KUA should		
	ecosystem.		
	authentication		
	made in the		
	when changes are		
	basis and as and		
	on half-yearly		
	personnel/entity,		
	induction of such		
	facilities, during		
	Authentication		
	Aadhaar		

20	Incident	AUA/KUA should				[]
29.	Incident		•	UIDAI		
	management	ensure that		Information		
	procedure	incident		Security		
	and RCA	management		Policy —		
	procedure	framework,		UIDAI		
		including forensic		External		
		investigation, is		Ecosystem —		
		implemented in		AUA/KUA —		
		accordance with		Section 2.12		
		the requirements		UIDAI		
		under UIDAI's	•	Information		
		Information				
		Security Policy		Security		
		and circulars.		Policy —		
				UIDAI		
		AUA/KUA should		External		
		perform Root		Ecosystem —		
		Cause Analysis		AUA KUA —		
		(RCA) for major		Section 2.13		
		incidents identified				
		in its ecosystem as				
		well as that of its				
		sub-contractors, if				
		any.				
30.	Incident	AUA/KUAshould	U	IDAI		
	reporting	ensure that the	In	formation		
	requirement	Sub-AUAs/Sub-	Se	curity Policy		
	for Sub-	KUAs, BCs and		- UIDAI		
	AUAs/Sub-	other sub-	Ex	xternal		
	KUAs and	contractors are	Ec	cosystem —		
	BCs	aware of Aadhaar		UA KUA —		
		authentication		ection 2.12		
		related incident	~ •			
		reporting.				
G.	Access contr					
31.	Multi-factor	AUA/KUA should	TT	IDAI		
51.		ensure in the case		formation		
		of assisted devices		curity Policy		
	n or operator	and applications		- UIDAI		
		where operators		xternal		
		-				
		need to		cosystem —		
		mandatorily		UA KUA —		
		perform	Se	ection 2.5		
		application				
		functions, that the				
		operator is				
		authenticated using				
		a multi-factor				

32.	Access provisioning mechanism	authentication scheme, such as user id, password, Aadhaar authentication, answer to personal security questions, soft token, hard token, one-time password, voice recognition, biometric data match and PIN. AUA/KUA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar processing related information.	 UIDAI Information Security Policy— UIDAI External Ecosystem— AUA KUA— Section 2.5 The Aadhaar (Data Security) Regulations, 2016— Clause (h) of regulation 5 		
33.	Privilege user access management	AUA/KUA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.			

24	Duint1-	ΑΤΤΑ /ΤΖΤΤΑ 1 11]
34.	Privilege	AUA/KUA should			
	accounts	ensure through the	Information		
		PAM tool that	Security Policy		
		privileged	— UIDAI		
		accounts, such as	External		
		NT Authority,	Ecosystem —		
		Administrator and	AUA KUA —		
		root accounts, are	Section 2.4		
		accessible only to			
		a limited set of			
		users, and			
		thataccess to			
		privileged account			
		is not allowed to			
		normal users.		 	
35.	Periodic	AUA/KUA should	• UIDAI		
	access	ensure that access	Information		
	review	is provided based	Security		
		on least privilege	Policy—		
		and that access is	•		
			UIDAI		
		reviewed	External		
		periodically (at	Ecosystem —		
		leasthalf-yearly).	AUA KUA —		
			Section 2.5 (2)		
			The Aadhaar		
			(Data		
			Security)		
			Regulations,		
			2016 —		
			Clause (h) of		
			regulation 5		
36.	Segregation	AUA/KUA should	-		
50.					
	of duties	ensure that	Information		
		personnel involved			
		in operational,	UIDAI External		
		development or	Ecosystem —		
		testing functions	AUA KUA —		
		should not be	Section 2.9(4)		
		given additional	and(5)		
		responsibilities in			
		system			
		administration			
		processes, audit			
		log maintenance,			
		security review of			
		-			
		system or			
		processes that may			

		compromise data			
		compromise data			
		security.			
		Where segregation			
		of duties is not			
		possible or			
		practicable, the			
		process should			
		include			
		compensating			
		controls, such as			
		monitoring of			
		activities,			
		maintenance and			
		review of audit			
		trails and			
		management			
		supervision.			
37.	Initial	AUA/KUA should	UIDAI		
	password	ensure that the	Information		
	allocation	allocation of initial	Security Policy		
	unocution	passwords is done	— UIDAI		
		in a secure manner	External		
		and that such	Ecosystem —		
		passwords are	AUA KUA —		
		changed on first	Section 2.6 (1)		
		login.			
38.	Password	AUA/KUA should	UIDAI		
	management	ensure that	Information		
	guidelines	passwords set are	Security Policy		
	guiaeimes	complex, with a	— UIDAI		
		-			
		minimum length of			
		eight characters	Ecosystem —		
		and—	AUA KUA —		
		(a) are not	Section 2.6 (5)		
		based on			
		anything			
		somebody			
		else may			
		easily			
		guess or			
		obtain			
		using			
		person			
		related			
		information			
		, e.g.,			
		,,	1		

Г Г Г			
	name,		
	telephone		
	number and		
	date of		
	birth;		
	(b) is free of		
	consecutive		
	identical		
	characters		
	or all-		
	numeric or		
	all-		
	alphabetica		
	l groups;		
	(c) contain at		
	least one		
	numeric,		
	one		
	uppercase		
	letter, one		
	lowercase		
	letter and		
	one special		
	character;		
	(d) are		
	required to		
	be changed		
	at regular		
	intervals		
	(passwords		
	for		
	privileged		
	accounts		
	should be		
	changed		
	more		
	frequently		
	than		
	normal		
	passwords);		
	(e) do not		
	allow the		
	use of the		
	last five		
	passwords;		
	(f) do not		
	allow the		

		username				
		and				
		password				
		to be the				
		same for a				
		particular				
		user; and				
		(g) do not use				
		the same				
		password				
		for various				
		UIDAI				
		access				
		needs of a				
		particular				
		user.				
39.	User	AUA/KUA should	UIDAI			
	account	ensure that three	Information			
	lockout	successive log-in	Security Policy			
		failures result in	— UIDAI			
		the user account	External			
		being locked. End	Ecosystem —			
		users / operators	AUA KUA —			
		should not be able	Section 2.5 (9)			
		to login until their				
		account is				
		unlocked and the				
		password is reset.				
40.	Restriction	AUA/KUA should	UIDAI			
	usage of	ensure that	Information			
	generic IDs	common or generic	Security Policy			
		or group user IDs	— UIDAI			
		are not used.	External			
			Ecosystem —			
			AUA KUA —			
			Section 2.5 (5)			
H.	Change man	agement				
41.	Change logs	AUA/KUA should	• UIDAI			
	management		Information			
		changes to	Security			
		Aadhaar	Policy —			
		authentication	UIDAI			
		applications,	External			
		infrastructure,	Ecosystem —			
		processes and	AUA KUA —			
		information	Section 2.15			
		processing	(1)			
L	1	- U		L	L	

		£			
		facilities, and	• UIDAI		
		maintain change	Information		
		log/register.	Security		
			Policy —		
			UIDAI		
			External		
			Ecosystem —		
			AUA KUA —		
			Section 2.15		
			(2)		
I.	Data security	y			
42.	Use of	AUA/KUA should	UIDAI		
	Aadhaar	ensure that if ADV	Guidelines for		
	data vault	is hosted on cloud,	ADV on Cloud		
	(ADV) on	the ADV cloud			
	cloud	service complies			
		with UIDAI's			
		Guidelines for			
		ADV on Cloud.			
		The ADV should			
		be hosted only by			
		Government			
		Community Cloud			
		(GCC) service			
		providers,			
		recognised as such			
		by the Ministry of			
		Electronics and			
		Information			
		Technology.			
43.	End-point	AUA/KUA should	UIDAI		
	security	ensure that USB	Information		
		access on the	Security Policy		
		servers and	— UIDAI		
		endpoints is, in the			
		default, restricted	Ecosystem —		
		for all, and the	AUA KUA —		
		same is allowed	Section 2.4		
		only on approval	500001 2.7		
		basis.			
44.	End-point	AUA/KUA should	UIDAI		
	security —	use licensed	Information		
	antivirus /	malware and	Security Policy—		
	anti-	antivirus solution	UIDAI External		
	malware	(preferablyNext-	Ecosystem —		
		Generation	AUA KUA —		
		antivirus) to	Section 2.9(10)		

		protect against			
		malware. The			
		malware/antivirus			
		installed should be			
		configured to			
		update in real time.			
45.	Use of	AUA/KUA and	UIDAI		
	security	ASA should ensure	Information		
	communicat	message security	Security Policy		
	ion	and integrity	— UIDAI		
	protocols	between their	External		
	•	servers and those	Ecosystem —		
		of third party	Section 2.11(6)		
		entities, such as			
		Sub-AUAs and			
		Sub-KUAs.			
		500 10713.			
		AUA/KUA should			
		procure digital			
		certificate from a			
		Certifying			
		Authority as			
		defined in the IT			
		Act.			
46.	End-point	AUA/KUA should	• UIDAI		
	security	ensure that end-	Information		
		point devices used	Security		
		for developing,	Policy —		
		process and	UIDAI		
		handling Aadhaar	External		
		data and	Ecosystem —		
		application timeout	AUA KUA —		
		after a session is	Section		
		idle for more than	2.9(29)		
		30 to 15 minutes,	• UIDAI		
		based on the	Information		
		criticality of the	Security		
		application.	Policy —		
			UIDAI		
			External		
			Ecosystem —		
			AUA KUA —		
			Section		
			2.9(30)		
			2.7(30)		

47	C]
47.	Secure	AUA/KUA should				
	software	implement system	Information			
	development	and processes to	Security Policy			
		ensure secure	— UIDAI			
		software	External			
		development	Ecosystem —			
		practices.	Section 2.9(5)			
		Periodic training of				
		developers should				
		be conducted on				
		secure software				
		development				
		practices. Records				
		of such trainings				
		should be				
		maintained.				
48.	Patch	AUA/KUA should	UIDAI			
	management	ensure that the	Information			
	6	patch management	Security Policy—			
		process is	UIDAI External			
		implemented for	Ecosystem —			
		applying patches to	•			
		information	Section 2.9(8)			
		systems. Patches				
		should be updated				
		at both the				
		application and the				
		server and network				
		levels.				
		AUA/KUA should				
		ensure that either				
		N or N-1 patches				
		are maintained.				
J.	Network sec	urity	I	L	I	
49.	Network	AUA/KUA should	UIDAI			
	security	ensure that Internet	Information			
		access on systems	Security Policy			
		are restricted to	— UIDAI			
		necessary or work-	External			
		related websites	Ecosystem —			
		and that access to	AUA KUA —			
		web portals known	Section 2.4			
		for pirated				
		software, gambling				
		etc. are restricted.				
L	1	1	1	1	1	

К.	Operations s	ecurity			
50.	Restrictions	AUA/KUA	UIDAI		
50.	on	personnel should	Information		
	designing/	not intentionally	Security Policy—		
	compiling	write, generate,	UIDAI External		
	malicious	compile, copy or	Ecosystem —		
	code	attempt to	AUA KUA —		
	code	introduce any	Section 2.9		
		computer code	Section 2.9		
		designed to			
		damage or			
		otherwise hinder			
		the performance			
		of, or access to,			
		any Aadhaar			
		information.			
51.	Implementat	AUA/KUA must	UIDAI circular		
51.	ion of	provide in their	no. K-		
	Virtual ID	authentication	11020/217/2018-		
	v Intuar ID		UIDAI (Auth-I),		
		application the option for an	dated 1.5.2018		
		Aadhaar number	(Implementation		
		holderto use a	of VID, UID		
		Virtual ID (VID)	Token and		
		for authentication,	Limited KYC)		
		in place of their	Linned KTC)		
		Aadhaar number.			
52.	Establishme	AUA/KUA should	Authoritor		
52.	nt of	have an effective	User Agency		
	grievance	grievance handling	Agreement		
	handling	mechanism and	version 6.0 —		
	mechanism	provide the same	Paragraph 14.3		
	mechanism	through multiple	r aragraph 14.3		
		channels.			
L.	Application				
		-			
53.	Compliance	AUA/KUA should	• The Aadhaar		
	to API	ensure that the	(Authenticatio		
	specification	**	n and Offline		
	s and	and software used	Verification)		
	application	for authentication	Regulations,		
	security	should conform to	2021 —		
		the latest API	Chapter II —		
		standards and	Sub-regulation		
		specifications laid	(2) of		
		down by UIDAI	regulation 8		
		from time to time,	and Chapter		
		and that itsSub-	III — Clause		

		(SDK) developed or digitally signed by the AUA/KUA.	 (a) of sub- regulation (3) of regulation 15 UIDAI Aadhaar Authentication Application Security Standard, version 1.0, 2020 UIDAI Aadhaar Authentication API Specification Version 2.5, Revision 1, January 2022 		
v a g i	-	ensure that it has	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(4)		
		ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of			

	T			ſ	[]
		API and			
		Distributed Denial			
		of Service (DDoS)			
		attacks.			
		AUA/KUA should			
		ensure that Cross-			
		Origin Resource			
		Sharing (CORS)			
		parameters are			
		configured to			
		restrict			
		unauthorised			
		domains from			
		accessing APIs			
		from the clientside.			
55.	Vulnerabilit	AUA/KUA should	UIDAI		
55.	y assessment		Information		
	y assessment	information	Security Policy		
		security policy,	— UIDAI		
		inclusive of	External		
		vulnerability assessment and	Ecosystem —		
			Section 2.10(6)		
		penetration testing			
		on its network, infrastructure and			
50		applications.			
56.		AUA/KUA should			
	n reviews	ensure that	Information		
	and system	authentication	Security Policy		
	walkthrough		— UIDAI		
		integrated with	External		
		IDAM, PIM/PAM	Ecosystem —		
		and SIEM.	Section 2.11(8)		
57.	Application	AUA/KUA should	UIDAI		
	code review	ensure that the	Information		
		passwords, tokens,	Security Policy		
		security keys and	— UIDAI		
		licenses are not	External		
		hardcoded in the	Ecosystem —		
		application code.	Section 2.10(5)		
М.	Logging and	monitoring			
58.	Clock	AUA/KUA should	• UIDAI		
	synchronisat		Information		
	ion through	Network Time	Security		
	use of	Protocol (NTP)	Policy—		
	Network	server of the	UIDAI		
				1	

	Time	National	External]
	Protocol	Informatics Centre	Ecosystem —			
	(NTP)	(NIC) or National	AUA KUA —			
		Physical	Section 2.9			
		-				
		Laboratory (NPL), or with NTP	(22)			
			• CERT-In			
		servers traceable to	Directive No.			
		the said NTP	20(3)/2022-			
		servers, for	CERT-In			
		synchronisation of	dated			
		all their ICT	28.4.2022			
		systems clocks.				
		Entities having				
		ICT infrastructure				
		spanning multiple				
		geographies may				
		also use accurate				
		and standard time				
		source other than				
		NPL and NIC;				
		however, it should				
		be ensured that				
		such time source				
		does not deviate				
		from NPL and				
N.	Droviding A	NIC. adhaar Authenticat	ion facilities to Sul	AUAg and Sub I		
59.	_	AUA/KUA should		J-AUAS allu Sull-1	NUAS	
59.			K11022/460/201			
	on	ensure that the authentication				
	application		6-UIDAI (Auth-			
	security	application to be	II), dated			
		used or being used	28.2.2017 -			
		for Aadhaar	Clause 1(i)			
		authentication by				
		its Sub-AUAs and				
		Sub-KUAs is				
		developed and be				
		digitally signed by				
		AUA/KUA.				
60.	Authenticati		UIDAI Circular			
	on	ensure that the	K11022/460/201			
	application	authentication	6-UIDAI (Auth-			
	security	application used by	II), dated			
		its Sub-AUAs and	28.2.2017 —			
		Sub-KUAs does	Clause 1(ii)			
		not store biometric				
1	1	data under any				

circumstance, and		
that the biometrics		
/ PID block is		
encrypted at the		
front-end device /		
client level.		

Compliance checklist for certifying compliance with controls that the AUA/KUA is required to have in place

Version 1.0 [issued in March 2024]

Important note: Wherever a control description requires AUA/KUA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablements are in place to secure compliance with the same on an ongoing basis.

Control no.	Short title	Control description	Control mapping	Compliance status (Compliant / Non- compliant / Not applicable)	Auditor's observation	Comments of AUA/KUA management
A.	Information secu				•	
1.	Security organisation and CISO function	AUA/KUA should ensure that it has a designated Chief Information Security Officer (CISO) function that oversees information security governance and compliances. The CISO should have independent reporting to its Board or other governing body or chief executive.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(1)			
2.	Appointment of management and technical single point of contact	AUA/KUA should appoint a Management Single Point of Contact (MPOC) and Technical Single Point of Contact (TPOC) that should oversee the management of the authentication	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

		application and			
		Aadhaar related			
		activities.			
		activities.			
		MPOC/TPOC			
		should ensure			
		consistent			
		communication			
		with UIDAI on			
		Aadhaar related			
		requirements and			
		compliances.			
		Any change in			
		MPOC/TPOC			
		should be			
		communicated to			
		UIDAI in a timely			
		manner.			
3.	Information	AUA/KUA should	UIDAI		
	security policy	have an	Information		
	and procedure	information	Security Policy		
		security policy and	—UIDAI		
		information	External		
		security procedures	Ecosystem —		
		in accordance with	AUA KUA —		
		industry leading	Section 2.9		
		standards, such as			
		ISO27001 (ISMS),			
		NIST Cyber			
		Security			
		Framework, CSA			
		Framework and			
		ISO27701 (PIMS).			
		The entity's			
		information			
		security policy			
		should also address			
		the security aspects			
		of Aadhaar, as			
		provided under the			
		Aadhaar Act,			
		regulations and			
		specifications.			

4.	Aadhaar	AUA/KUA should	UIDAI		
	authentication	ensure that the	Information		
	application	authentication	Security Policy		
	design	application design	—UIDAI		
	8	architecture is	External		
		documented and	Ecosystem —		
		validated by	Section 2.3(5)		
		UIDAI Technology	50000012.5(5)		
		Centre and covers			
		Aadhaar security			
		requirements.			
5.	Aadhaar	AUA/KUA should	UIDAI		
5.	authentication	ensure that the	Information		
	application	Aadhaar data flow	Security Policy		
	design		— UIDAI		
	design	is properly documented for its	External		
		AUA/KUA			
			Ecosystem —		
		applications and those of its Sub-	Section 2.3(6)		
		AUAs and Sub-			
		KUAs.			
6.	Risk assessment	AUA/KUA should	UIDAI		
0.	Risk assessment		Information		
		implement process			
		and procedure to	Security Policy — UIDAI		
		perform periodic	External		
		(at least annual) information			
		security risk	Ecosystem —		
		assessment of its	Section 2.3(13)		
		ICT infrastructure			
		supporting the authentication			
		application.			
		Further, entity			
		should also			
		perform risk			
		assessment of its			
		third party			
		suppliers / vendors			
		having access to the Aadhaar			
		application and the data of Aadhaar			
		number holders.			
		Security risks			
	1		1	1	

	1		1	1	[,
		should be				
		documented and				
		reviewed				
		periodically by				
		Security Officers /				
		CISO / those in				
		charge of the				
		security				
		governance of the				
		AUA/KUA and its				
		Sub-AUAs and				
		Sub-KUAs.				
7.	Third party	AUA/KUA should	UIDAI			
1.						
	information	ensure that it has a	Information			
	security policy	third party	Security Policy			
		information	— UIDAI			
		security policy that	External			
		lays down the	Ecosystem —			
		security controls	Section 2.3(14)			
		and compliances	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
		that its third party				
		vendors, suppliers,				
		ICT service				
		providers and ICT				
		support vendors				
		(<i>e.g.</i> , third party /				
		outsource				
		application				
		developers,				
		-				
		infrastructure				
		support vendors,				
		data centre hosting				
		agency, cloud				
		service providers				
		etc.) are obligated				
		to adhere to.				
В.	Compliance requ					
		1		1	1	
8.	IPR provisions	The AUA/KUA	Authentication			
	contained in	should be in	User Agency			
	UIDAI's	compliance with	Agreement			
	Aadhaar User	the intellectual	version 6.0 —			
	Agency	property provisions	Section 3			
	Agreement	contained in				
	(latest version)	UIDAI's Aadhaar				
	(101051 10151011)					
		User Agency				
1	1	Agreement (latest	1	1	1	
		version).				

9. Annual AUAKUA should • The Aadhaar (Authenticati o and (Authenticati o and Offline empanelled by an information systems audited by an information systems audited or need basis to ensure compliance ensure compliance specifications. The adhaar gecilitations. The adhaar (Data Stauld report should be shared with UIDAI's standards and specifications. The adhaar (Data Stauld report should be shared with UIDAI's standards and specifications. The adhaar (Data AUAKUA Bubber) (I) of regulation, 2016 • UIDAI from aton so avoid recurrece of the audit, AUAKUA Sthould— (e) determine the causes of the audit, Bubber (I) evaluate the need for actions to avoid recurrece of the same; (g) determine and enforce the implementation a of corrective actions to ake (I) evaluate the need for actions; and (I) review the corrective actions taken.						
The annual audit	9.	security audit by CERT-In- empanelled	operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with UIDAI's standards and specifications. The audit report should be shared with UIDAI. If any non- compliance is found as a result of the audit, AUA/KUA should— (e) determine the causes of the non- compliance; (f) evaluate the need for actions to avoid recurrence of the same; (g) determine and enforce the implementatio n of corrective and preventive actions; and (h) review the corrective actions taken.	on and Offline Verification) Regulations, 2021 — Chapter III — Clause (h) of sub- regulation (1) of regulation 14 • The Aadhaar (Data Security) Regulations, 2016 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section		
should cover all			should cover all			

		security controls			
		applicable under			
		the Aadhaar (Data			
		Security)			
		Regulations, 2016.			
10.	Onboarding of	AUA/KUA should	The Aadhaar		
	ASA	ensure that UIDAI	(Authentication		
		is informed of the	and Offline		
		ASAs with whom	Verification)		
		it has entered into	Regulations,		
		agreement to	2021 — Chapter		
		provide necessary	III — Sub-		
		infrastructure for	clause (g) of		
		ensuring secure network	sub-regulation		
		connectivity and	(1) of regulation 14		
		related services to	14		
		it to enable			
		performance of			
		authentication			
		using the			
		Authentication			
		facilities provided			
		by UIDAI.			
11.	Annual	AUA/KUA should	UIDAI		
	compliance	ensure that the	Information		
	audit of Sub-	operations and	Security		
	AUAs and Sub-	systems of its Sub-	Policy—UIDAI		
	KUAs	AUAs and Sub-	External		
		KUAs are audited	Ecosystem —		
		on an annual basis	AUA KUA —		
		by an information	Section 2.13		
		systems auditor certified by a			
		recognised body, to			
		ensure compliance			
		with such standards			
		and specifications			
		as UIDAI may			
		specify from time			
		to time and that the			
		audit report is			
		shared with			
		UIDAI.			
C.	Data privacy				

10	Dete muste etiem			
12.	Data protection	AUA/KUA should	• UIDAI	
	policy	establish a data	Information	
		protection policy	Security	
		addressing, inter	Policy —	
		alia, data protection	UIDAI	
		related aspects	External	
		under—	Ecosystem —	
		(d) the Aadhaar	AUA/KUA	
		Act, the	— Section	
		regulations	2.14(2)	
		made	• The IT Act	
		thereunder and	• Till the	
		the standards	coming into	
		and	force of the	
		specifications	DPDP Act,	
		issued by	the SPDI	
		UIDAI from	Rules and, on	
		time to time;	and from the	
		(e) the	date of	
		Information	coming into	
		Technology	force of	
		Act, 2000 ("IT	clauses (a)	
		Act"); and	and (c) of	
		(f) till the coming	sub-section	
		into force of	(2) of section	
		the Digital	44 of the	
		Personal Data	DPDP Act,	
		Protection	the said Act	
		Act, 2023	and the rules	
		("DPDP	made	
		Act"), the	thereunder ¹³	
		Information	lifereunder	
		Technology		
		(Reasonable		
		Security		
		Practices and		
		Procedures		
		and Sensitive		
		Personal Data		
		Or Information)		
		Information)		
		Rules, 2011		
		("SPDI		
		Rules") and,		
		on and from		

	1		r		,
		the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of AUA/KUA and the URL for the same should be			
13.	Consent of Aadhaar number	mentioned. The AUA/KUA should obtain	The Aadhaar (Authentication		
	holder	consent of the Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, before collecting their identity information for the purposes of authentication. The consent should be obtained preferably in electronic form.	and Offline Verification) Regulations, 2021 — Chapter II — Regulation 6		
14.	Information to Aadhaar number holder on the nature of information that will be shared upon	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or,	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause (a)		
	performance of authentication	in case of a child, the parent or legal guardian of such child, regarding the nature of information that will be shared by	of sub- regulation (1) of regulation 5		

		UIDAI upon			
		performance of			
		authentication.			
15			TT1 A 11		
15.	Information to	At the time of	The Aadhaar		
	Aadhaar number	authentication,	(Authentication		
	holder on use of	before obtaining	and Offline		
	information	consent,	Verification)		
	received during	AUA/KUA should	Regulations,		
	authentication	inform the Aadhaar	2021 — Chapter		
		number holder or,	II — Clause (b)		
		in case of a child,	of sub-		
		the consent of the	regulation (1) of		
		parent or legal	regulation 5		
		guardian of such			
		child, of the uses to			
		which the			
		information			
		received during			
		authentication may			
		be put to by it.			
16.	Alternative	At the time of	The Aadhaar		
10.	mechanisms for	authentication,	(Authentication		
	submission of	before obtaining	and Offline		
		e e	Verification)		
	identity information	consent, AUA/KUA should	,		
	mormation		Regulations,		
		inform the Aadhaar	2021 - Chapter		
		number holder or,	II - Clause (c)		
		in case of a child,	of sub-		
		the parent or legal	regulation (1) of		
		guardian of such	regulation 5		
		child, of the			
		alternatives to			
		submission of			
		identity			
		information.			
17.	Consent	The AUA/KUA	• The Aadhaar		
	communication	should ensure that	(Authenticati		
	in local	the consent	on and		
	language	information is	Offline		
		communicated in	Verification)		
		local language.	Regulations,		
			2021 —		
		The AUA/KUA	Chapter II —		
		should also ensure	Sub-		
		that, on and from	regulation (2)		
		the date of coming	of regulation		
		into force of sub-	5		
		mo force of sub-	5		

[0.10		
		section (3) of	• On and from		
		section 5 of the	the date of		
		DPDP Act, the	coming into		
		Aadhaar number	force of sub-		
		holder has the	section (3) of		
		option to access the	section 5 and		
		contents of the	sub-section		
		notice referred to in	(3) of section		
		sub-sections (1)	6 of the		
		and (2) of the said	DPDP Act,		
		section and the	the said Act		
		request for consent	— Sub-		
		referred to in sub-	section (3) of		
		section (3) of	section 5 and		
		section 6in English	sub-section		
		or any language	(3) of section		
		specified in the	6		
		Eighth Schedule to			
		the Constitution.			
18.	Communication	The AUA/KUA	UIDAI		
	of consent	should make	Information		
	related	provisions for	Security Policy		
	information to	communication of	— UIDAI		
	persons with	consent related	External		
	visual/hearing	information to	Ecosystem —		
	disability	persons with	AUA/KUA —		
	5	visual/hearing	Section 2.14		
		disability in an			
		appropriate			
		manner.			
19.	Consent log	AUA/KUA should	• The Aadhaar		
	retention	maintain the logs	(Authenticati		
	-	for—	on and		
		(a) record of	Offline		
		consent of	Verification)		
		the Aadhaar	Regulations,		
		number	2021 —		
		holder for	Chapter II —		
		authenticati	Sub-		
		on; and	regulation		
		(b) record of	(2) of		
		disclosure	regulation 6		
		of	 The Aadhaar 		
		information	• The Aadhaar (Authenticati		
		, as	on and		
		mentioned	Offline		
		in Control			
			Verification)		

[]					1	
		numbers 13,		Regulations,		
		14, 15, 16,		2021 —		
		17 and 18		Chapter III		
		above, to		— Clause (d)		
		the Aadhaar		of sub-		
		number		regulation		
		holder at		(1) of		
		the time of		regulation 18		
		authenticati	•			
		on.		Information		
				Security		
		For any given		Policy —		
		Aadhaar number		UIDAI		
		holder, whose		External		
		identity		Ecosystem		
		information was		— AUA		
		collected, the		KUA —		
		AUA/KUA should		Section 2.14		
		be able to		Section 2.14		
		demonstrate that				
		consent was taken				
		and disclosure of				
		information was				
• •		made.				
20.	Explicit consent;	AUA/KUA should	•	UIDAI		
	no umbrella	ensure that the		Information		
	consent	consent taken from		Security		
		the Aadhaar		Policy —		
		number holder		UIDAI		
		should in		External		
		accordance with		Ecosystem —		
		the provisions of		AUA/KUA		
		the Aadhaar Act,		— Section		
		2016 and the		2.9		
		regulations made	•	On and from		
		thereunder;no		the date of		
		umbrella consent		coming into		
		should be taken for		force of sub-		
		sharing e-KYC or		section (1) of		
		Aadhaar number of		section 5 and		
		the Aadhaar		sub-section		
		number holders		(1) of section		
		with other entities.		6 of the		
				DPDP Act,		
		The AUA/KUA		the said Act		
		should also ensure		— Sub-		
				540-	1	
		that, on and from		section (1) of		

					I
		the date of coming	section 5 and		
		into force of sub-	sub-section		
		section (1) of	(1) of section		
		section 5 and sub-	6		
		section (1) of			
		section 6 of the			
		DPDP Act, the			
		consent taken from			
		the Aadhaar			
		number holder is in			
		accordance with			
		the applicable			
		provisions of			
		sections 5 and 6 of			
		the said Act.			
D.	Asset manageme	nt			
21.	Biometric	AUA/KUA should	• The Aadhaar		
	device	capture the	(Authenticati		
	management	biometric	on and		
	U	information of the	Offline		
		Aadhaar number	Verification)		
		holder using	Regulations,		
		certified and	2021 —		
		registered	Chapter II —		
		biometric devices	Clause (a) of		
		as per standards	sub-		
		specified by UIDAI			
			regulation (1)		
		from time to time.	of regulation		
			7, sub-		
			regulation (1)		
			of regulation		
			8 and clause		
			(d) of sub-		
			regulation (1)		
			of regulation		
			14		
			• UIDAI		
			Information		
			Security		
			Policy —		
			UIDAI		
			External		
			Ecosystem —		
			AUA/KUA		
			— Section		
			2.4		

22.	Biometric	Devices	Advisory		
	device	reportingtransactio	regarding		
	management	ns at a very low	strengthening of		
	C	frequency over	Biometric		
		time may be	authentication		
		potential targets of	security		
		frauds. Therefore,	[Advisory F. no.		
		AUA/KUA should	13043/2/2021-		
		maintain oversight	AUTH-1-HQ,		
		in respect of the	dated 31.5.2022]		
		same and identify			
		and remove such			
		devices from the			
		system.			
23.	Biometric	AUA/KUAshould	The Aadhaar		
	device	monitor the	(Authentication		
	management	operations of its	and Offline		
		devices and	Verification)		
		equipment, on	Regulations,		
		periodic basis, for	2021 — Chapter		
		compliance with	III — Clause (e)		
		the terms and	of sub-		
		conditions,	regulation (1) of		
		standards,	regulation 14		
		directions and			
		specifications, issued and			
		communicated by UIDAI from time			
		to time.			
24.	Biometric	AUA/KUAshould	Advisory		
	device	carryout analysis of	regarding		
	management	devices with high	strengthening of		
	C	failure rates and	biometric		
		replace them.	authentication		
		•	security		
			[Advisory F. no.		
			13043/2/2021-		
			AUTH-1-HQ,		
			dated 31.5.2022]		
25.	End-point	AUA/KUA should	Advisory		
	security	ensure that	regarding		
		biometric	strengthening of		
		deploying devices	Biometric		
		are connected with	authentication		
		end-point systems	security		
		that have the latest	[Advisory F. no.		

			12042/2/2021		
		operating system	13043/2/2021-		
		(OS) specifications	AUTH-1-HQ,		
		(as of March 2024,	dated 31.5.2022]		
		at least Windows			
		10 and above and			
		Android OS 10 and			
		above), and that			
		systems based on			
		an OS that is end-			
		of-life or end-of-			
		support are not			
		deployed or used.			
26.	Security	AUA/KUA should	UIDAI		
	hardening of	ensure all the end-	Information		
	assets	point devices and	Security Policy		
		assets are used only	— UIDAI		
		after hardening to	External		
		reduce/eliminate			
			Ecosystem —		
		the attack vector	AUA KUA —		
		and condense the	Section 2.4		
		system attack			
		surface.			
27.	Asset inventory	AUA/KUA should	UIDAI		
	maintenance	ensure that all	Information		
		assets (business	Security		
		applications,	Policy—UIDAI		
		operating systems,	External		
		databases, network			
			Ecosystem —		
		etc.) used for the	AUA KUA —		
		purpose of	Section 2.4		
		delivering services			
		to Aadhaar number			
		holders using			
		Aadhaar			
		Authentication			
		facilitiesare			
		identified, labelled			
		and classified.			
		AUA/KUA should			
		record the details			
		regarding assets			
		used and maintain			
		and update the			
		asset inventory on			
		a continuous basis.			
		Ownership of			
L					

28.	Maintenance of software inventory	authentication assets should be clearly documented. AUA/KUA should ensure that it uses only licensed	UIDAI Information Security Policy		
		software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.	— UIDAI External Ecosystem — AUA KUA — Section 2.13		
29.	Asset disposal procedure	AUA/KUA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposed of securely.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.4		
30.	Asset repair procedure and asset movement logs	AUA/KUA should, before consigning any asset for repair, sanitise the same to ensure that it does not contain any Aadhaar related data. A register to log the movement of all the assetsconsigned outside should be maintained.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.4		
31.	Asset repair procedure	AUA/KUA should, in case of in-house repair of assets,	UIDAI Information Security Policy -		

		1			
		document the	UIDAI External		
		details of the	Ecosystem —		
		original equipment	AUA KUA —		
		manufacturer (OE	Section 2.4		
		M) and maintain			
		the logs of the			
		assets being			
		repaired.			
Ε.	Human resource				
32.	Background	AUA/KUA should	UIDAI		
	verification and	conduct a	Information		
	signing of	background check	Security Policy		
	confidentiality	and sign a	—UIDAI		
	agreement	confidentiality	External		
	agreement	agreement / non-	Ecosystem —		
		disclosure	AUA KUA —		
		agreement (NDA)	Section 2.3		
		with all			
		personnel/agency			
		handling Aadhaar			
		related information.			
		Access to			
		authentication			
		infrastructure			
		should not be			
		granted before			
		signing NDA and			
		completion of			
		background			
		verification (BGV)			
		for personnel.			
33.	Background	AUA/KUA should	UIDAI	<u> </u>	<u> </u>
	verification and	take an undertaking	Information		
	signing of	from business	Security Policy		
			—UIDAI		
	confidentiality	correspondents			
	agreement with	(BCs) and similar	External		
	third-party	entities, Sub-	Ecosystem —		
	contractors	AUAs/Sub-KUAs	AUA KUA —		
		and other third	Section 2.3		
		party contractors			
		regarding NDAs			
		and BGVs			
		conducted			
		successfully for			
		their personnel			
		handling Aadhaar			
		related data.			
		Totatoo Gata.			

34.	Training and	AUA/KUA should	UIDAI		
54.	awareness	ensure that MPOC,	Information		
	awareness	TPOC and their	Security Policy		
			— UIDAI		
		supporting teams			
		that manage and	External		
		maintain the	Ecosystem —		
		authentication	Section 2.3(7)		
		application and its			
		underlying			
		infrastructure, are			
		aware of Aadhaar			
		security			
		requirements.			
35.	Operator	AUA/KUA should	The Aadhaar		
	qualification	ensure that the	(Authentication		
		operator employed	and Offline		
		for performing	Verification)		
		authentication	Regulations,		
		functions and	2021 — Chapter		
		maintaining	III — Clause (f)		
		necessary systems,	of sub-		
		infrastructure and	regulation (1) of		
		process, possess	regulation 14		
		requisite	C		
		qualification for			
		undertaking such			
		work.			
36.	Periodic	AUA/KUA should	UIDAI		
2 0.	information	impart information	Information		
	security and	security and data	Security Policy		
	privacy trainings	privacy trainings to	—UIDAI		
	related to	all its personnel as	External		
	Aadhaar	well as those of any	Ecosystem —		
	authentication	BCs, Sub-	AUA KUA —		
		AUAs/Sub-KUAs			
	operations		Section 2.3		
		and similar entities,			
		in relation to the			
		use of Aadhaar			
		Authentication			
		facilities, during			
		induction of such			
		personnel/entity, on			
		half-yearly basis			
		and as and when			
		changes are made			
		in the			
		authentication			

acconstant	
ecosystem.	
AUA/KUA should	
further ensure that	
specific and	
specialised training	
are imparted for	
various functional	
roles involved in	
the authentication	
ecosystem and that	
the same cover all	
relevant security	
and data privacy	
guidelines, as per	
the UIDAI	
Information	
Security Policy for	
Authentication,	
Aadhaar Act, 2016	
and the regulations	
made thereunder	
and circulars,	
notices etc. issued	
by UIDAI from	
time to time.	
AUA/KUA should	
also maintain a	
record of such	
trainings imparted.	
F. Incident management	
37. Incident AUA/KUA should • UIDAI	
management ensure that incident Information	
procedure and management Security	
RCA procedure framework, Policy—	
including forensic UIDAI	
investigation, is External	
implemented in Ecosystem —	
accordance with AUA/KUA	
the requirements — Section	
under UIDAI's 2.12	
Information • UIDAI	
Security Policy and Information	
circulars. Security	
AUA/KUA should Policy —	

		perform Root		UIDAI		
		Cause Analysis		External		
		(RCA) for major				
		incidents identified		Ecosystem —		
				AUA KUA — Section		
		in its ecosystem as well as that of its				
				2.13		
		sub-contractors, if				
20		any.				
38.	Reporting of	AUA/KUA	•	The Aadhaar		
	incidents to	should—		(Authenticati		
	UIDAI and	(a) inform		on and		
	CERT-In	UIDAImisuse		Offline		
		of any		Verification)		
		information or		Regulations,		
		systems		2021 —		
		related to the		Chapter III		
		Aadhaar		— Clause (l)		
		framework or		of sub-		
		any		regulation		
		compromise of		(1) of		
		Aadhaar		regulation 14		
		related	•	UIDAI		
		information or		Information		
		systems within		Security		
		its network,		Policy —		
		and report any		UIDAI		
		confidentiality		External		
		security		Ecosystem		
		breach of				
		Aadhaar		AUA/KUA		
		related		— Item 4 of		
		information to		section 2.12		
		UIDAI within	•	Directions		
		24 hours;		dated		
		(b) report cyber		28.4.2022 of		
		incidents as		CERT-In,		
		mentioned in		bearing no.		
		Annexure I to		20(3)/2022-		
		the directions		CERT-In —		
		dated		Clause (ii)		
		28.4.2022 of	•	DPDP Act		
		CERT-In,		— Sub-		
		bearing no.		section (6) of		
		20(3)/2022-		section 8 and		
		CERT-In,		the rules		
		within 6 hours		under clause		
		of noticing		(f) of sub-		
				(1) 01 500-		

		such incidents	section (2) of			
		or the same	section (2) of section 40			
			section 40			
		being brought				
		to their notice;				
		and				
		(c) on and from				
		the date of				
		coming into				
		force of sub-				
		section (6) of				
		section 8 of				
		the DPDP Act,				
		intimation of				
		personal data				
		breach to the				
		Board and				
		each affected				
		Data Principal,				
		within such				
		time as may be				
		prescribed by				
		rules made				
		under the said				
		Act.				
39.	Incident	AUA/KUA should	UIDAI			
	reporting	ensure that the	Information			
	requirement for	Sub-AUAs/Sub-	Security Policy			
	Sub-AUAs/Sub-	KUAs, BCs and	— UIDAI			
	KUAs and BCs	other sub-	External			
		contractors are	Ecosystem —			
		aware of Aadhaar	AUA KUA —			
		authentication	Section 2.12			
		related incident				
		reporting.				
G.	Access control					
40.	Multi-factor	AUA/KUA should	UIDAI			
	authentication of	ensure in the case	Information			
	operator	of assisted devices	Security Policy			
		and applications	— UIDAI			
		where operators	External			
		need to	Ecosystem —			
		mandatorily	AUA KUA —			
		perform application	Section 2.5			
		functions, that the				
		operator is				
		authenticated using				
		a multi-factor				
	1	L	l	L	l	

				I	
		authentication			
		scheme, such as			
		user id, password,			
		Aadhaar			
		authentication,			
		answer to personal			
		security questions,			
		soft token, hard			
		token, one-time			
		password, voice			
		recognition,			
		biometric data			
		match and PIN.			
41.	Operator logs	AUA/KUA should	Advisory		
41.	Operator logs		-		
		maintain details of	regarding		
		devices and	strengthening of		
		operators employed	biometric		
		for the use of	authentication		
		Aadhaar	security		
			•		
		Authentication	[Advisory F. no.		
		facilities in assisted	13043/2/2021-		
		mode, including	AUTH-1-HQ,		
		proper logs of such	dated 31.5.2022]		
		operators, along			
		with their name,			
		deviceID, date and			
		time, etc. These			
		logs should be			
		verified by			
		•			
		AUA/KUA at			
		regular intervals.			
42.	Access	AUA/KUA should	• UIDAI		
	provisioning	ensure that only	Information		
	mechanism	authorised	Security		
	meenumon	individuals are able	-		
			Policy —		
		to access	UIDAI		
		information	External		
		facilities such as	Ecosystem —		
		the authentication	AUA KUA		
		application, audit	— Section		
		logs, authentication	2.5		
		servers,	• The Aadhaar		
		application, source	(Data		
		code, information	Security)		
		security	Regulations,		
		•	•		
		infrastructure, etc.,	2016 —		
		and Aadhaar	Clause (h) of		

		processing related information.	regulation 5		
43.	Privilege user access management	AUA/KUA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (6)		
44.	Privilege accounts	AUA/KUA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator and root accounts, are accessible only to a limited set of users, and thataccess to privileged account is not allowed to normal users.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4		
45.	Periodic access review	AUA/KUA should ensure that access is provided based on least privilege and that access is reviewed periodically (at least half-yearly).	 UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (2) The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of regulation 5 		

46.	Access	Within 24 hours of	UIDAI		
0.	revocation	exit of any	Information		
	mechanism	personnel,	Security		
	meenamsm	AUA/KUA should	Policy—UIDAI		
		revoke the rights	External		
		and privileges to	Ecosystem —		
			AUA KUA —		
		access or process Aadhaar related			
			Section 2.3(8)		
		information. Upon	and section 2.5		
		such revocation,			
		user IDs should be			
		deleted forthwith if			
47		not in use.			
47.	Segregation of	AUA/KUA should	UIDAI		
	duties	ensure that	Information		
		personnel involved	Security Policy		
		in operational,	— UIDAI		
		development or	External		
		testing functions	Ecosystem —		
		should not be given	AUA KUA —		
		additional	Section		
		responsibilities in	2.9(4)and(5)		
		system			
		administration			
		processes, audit log			
		maintenance,			
		security review of			
		system or processes			
		that may			
		compromise data			
		security.			
		Where segregation			
		of duties is not			
		possible or			
		practicable, the			
		process should			
		include			
		compensating controls, such as			
		monitoring of			
		activities,			
		maintenance and			
		review of audit			
		trails and			
		management			
		supervision.			
		supervision.			

48.	Initial password	AUA/KUA should	UIDAI		
40.	allocation	ensure that the	Information		
	anocation	allocation of initial			
			Security Policy — UIDAI		
		passwords is done	External		
		in a secure manner			
		and that such	Ecosystem —		
		passwords are	AUA KUA —		
		changed on first	Section 2.6 (1)		
40		log in.			
49.	Password	AUA/KUA should	UIDAI		
	management	ensure that	Information		
	guidelines	passwords set are	Security Policy		
		complex, with a	— UIDAI		
		minimum length of	External		
		eight characters	Ecosystem —		
		and—	AUA KUA —		
		(h) are not	Section 2.6 (5)		
		based on			
		anything			
		somebody			
		else may			
		easily guess			
		or obtain			
		using			
		person			
		related			
		information			
		, <i>e.g.</i> , name,			
		telephone			
		number and			
		date of			
		birth;			
		(i) is free of			
		consecutive			
		identical			
		characters			
		or all-			
		numeric or			
		all-			
		alphabetical			
		groups;			
		(j) contain at			
		least one			
		numeric,			
		one			
		uppercase			
		letter, one			
L	1	2		1	

lowercase letter and one special character; (k) are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords; (1) do not allow the use of the last five passwords; (moto ot allow the username and password to be the same for a particular
one special character; (k) are required to be changed at regular intervals (passwords for privileged accounts accounts should be changed more frequently than normal passwords; (1) do not allow the use of the last five passwords; and and be the same internance and and aparticular internance and internance and internance and internance and internance and internance and internance and internance and internance and
character; (k) are required (k) are required intervals changed at regular intervals intervals (passwords intervals for privileged accounts intervals should be intervals changed intervals more intervals frequently than normal passwords); intervals (1) do not allow the last five passwords; (m)do not allow the attrive asswords; (m)do not allow the and passwords; image and passwords intervals image and passwords intervals image and passwords intervals image intervals image intervals image intervals image intervals image intervals image intervals <
(k) are required to be to be changed at regular regular intervals (passwords for privileged accounts should be changed acounts should be acounts should be acounts gasswords); acounts (1) do not anore gasswords); (1) do not allow the use of the last five passwords; (modo not allow the username and and password to be the same for a particular particular
to be changed at cchanged at regular regular intervals (passwords) (passwords) privileged accounts should be accounts should be accounts requently than normal passwords); allow the use of the allow the username and allow the and username and password to be the same for a particular
changed at regular intervals (passwords for privileged accounts accounts should be accounts changed more more for gasswords); (1) do not allow the use of the last five passwords; (m)do not allow the allow the use of the allow the allow the use of the allow the allow the strive passwords; interval (m)do not allow the and password to be the same interval interval and password to perticular
regular intervals $(passwords)$ for privileged accounts should be changed more frequently than normal passwords); $ $
regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords); (1)do not allow the use of the last five passwords; (m)do not allow the username and password to be the same for a particular
intervalsintervals(passwordsintervalsforprivilegedaccountsintervalsshould beintervalschangedintervalsmoreintervalsfrequentlyintervalsthan normalintervalspasswords);intervals(1)do notallow theintervalsuse of theintervalslast fiveintervalspasswords;intervals(m) do notintervalsallow theintervalsusernameintervalsandintervalspassword tointervalsbe the sameintervalsfor aparticular
(passwords for privileged accounts should be changed more frequently than normal passwords);
forprivilegedaccountsshould bechangedmorefrequentlythan normalpasswords);(1) do notallow thelast fivepasswords;(m)do notallow theuse of thelast fivepasswords;(m)do notallow theusernameandpassword tobe the samefor aparticular
privileged accounts should be changed more frequently than normal passwords); (1) do not allow the last five passwords; (m)do not allow the use of the last five passwords; (m)do not allow the username and password to be the same for a particular
accounts should be changed more frequently than normal passwords); (1) do not allow the use of the last five passwords; (m)do not allow the username and password to be the same for a particular
should be changed more more frequently than normal passwords); intervention (1) do not allow the use of the last five passwords; intervention (m)do not allow the username and password to be the same for a particular
changed moremorefrequently than normal passwords);iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii
morefrequentlythan normalpasswords);(1) do notallow theuse of thelast fivepasswords;(m) do notallow theusernameandpassword tobe the samefor aparticular
frequently than normal passwords);Image: Constant of the passwords);(1) do not allow the use of the last five passwords;Image: Constant of the passwords;(m)do not allow the usernameImage: Constant of the password to be the same for a particular
than normal passwords);
passwords);(1) do notallow theuse of thelast fivepasswords;(m)do notallow theusernameandpassword tobe the samefor aparticular
(1) do not allow the allow the use of the last five passwords; (m)do not allow the allow the username and password to be the same for a for a particular
allow the use of the use of the last five passwords; passwords; (m)do not allow the allow the username and password to be the same interformant for a particular
use of the last five passwords; (m)do not allow the username and be the same for a particular1
last five passwords; (m)do not allow the username and1ipassword to be the same for a particular1
passwords; (m)do not allow the username and password to be the same for a particularImage: Comparison of the same of
(m)do notallow theusernameandpassword tobe the samefor aparticular
allow the usernameandpassword tobe the samefor aparticular
usernameandpassword tobe the samefor aparticular
and password to password to password to be the same particular
password to be the same for a particular
password to be the same for a particular
be the same for a particular
for a particular
particular
user and
user; and (a) do not use
the same
password for various
for various
UIDAI
access
needs of a
particular
user.
50. User account AUA/KUA should UIDAI
lockout ensure that three Information
successive log-in Security Policy
failures result in — UIDAI
the user account External

		1 • 1 1 1 1 1	D (
		being locked. End	Ecosystem —		
		users / operators	AUA KUA —		
		should not be able	Section 2.5 (9)		
		to log in until their			
		account is unlocked			
		and the password is			
		reset.			
51.	Restriction	AUA/KUA should	UIDAI		
	usage of generic	ensure that	Information		
	IDs	common or generic	Security Policy		
		or group user IDs	— UIDAI		
		are not used.	External		
			Ecosystem —		
			AUA KUA —		
			Section 2.5(5)		
H.	Change manager	nent		1	L
52.	Change logs	AUA/KUA should	• UIDAI		
52.	management	document all	Information		
	management	changes to Aadhaar	Security		
		authentication	Policy —		
		applications,	UIDAI		
		infrastructure,	External		
		,			
		processes and	Ecosystem —		
		information	AUA KUA		
		processing	— Section		
		facilities, and	2.15(1)		
		maintain change	• UIDAI		
		log/register.	Information		
			Security		
			Policy —		
			UIDAI		
			External		
			Ecosystem —		
			AUA KUA		
			— Section		
			2.15(2)		
I.	Physical security	r			
53.	Physical	AUA/KUA data	UIDAI		
	security of AUA	centre hosting	Information		
	data centre	Aadhaar related	Security		
		information should	Policy—UIDAI		
		be secured fully	External		
		and should have	Ecosystem —		
		access control.	AUA KUA —		
			Section 2.8		
54.	Security of	AUA/KUA should	UIDAI		
51.	Security of			1	

	AUA servers	ensure that their	Information		
	HON SCIVEIS	servers are placed	Security		
		in an isolated,	Policy—UIDAI		
		secure cabinet in	External		
		the data centre.			
		the data centre.	Ecosystem —		
			AUA KUA —		
			Section 2.8		
55.	Physical	AUA/KUA data	UIDAI		
	security of	centre and servers	Information		
	AUA/KUAdata	should be under	Security		
	centre	24X7protection of	Policy—UIDAI		
		security guards and	External		
		CCTV	Ecosystem —		
		surveillance.	AUA KUA —		
			Section 2.8		
56.	Physical	AUA/KUA should	UIDAI		
	security of	ensure that access	Information		
	AUA/KUA data	to the data centre is	Security		
	centre	restricted only to	Policy—UIDAI		
		authorised	External		
		individuals and	Ecosystem —		
		appropriate logs of	AUA KUA —		
		entry of individuals	Section 2.8		
		should be	Section 2.0		
		maintained.			
57.	Dhysical	AUA/KUA should	UIDAI		
57.	Physical security of		Information		
	5	ensure that physical			
		access to the data	Security		
	centre	centre and other	Policy—UIDAI		
		restricted areas	External		
		hosting critical	Ecosystem —		
		Aadhaar related	AUA KUA —		
		equipment/informat	Section 2.8		
		ion is pre-approved			
		and recorded, along			
		with the date, time			
		and purpose of			
		entry.			
58.	Physical	AUA/KUA should	UIDAI		
	security of	ensure that the	Information		
	AUA/KUA data	movement of all	Security		
	centre	incoming and	Policy—UIDAI		
		outgoing assets	External		
		related to Aadhaar	Ecosystem —		
		in the AUA/KUA	AUA KUA —		
		data centre is	Section 2.8		
			Section 2.8		
		documented.			

59.	Physical	AUA/KUA should	UIDAI		
	security of AUA/KUA data centre	ACA/KCA should ensure that visible and clearly readable signs/notices notifying areas designated as restricted areas and provisions restricting entry to the same are posted at all points leading to entry to such areas.	Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8		
60.	Physical security of AUA/KUA data centre	AUA/KUA should provide lockable cabinets or safes in the data centre and information processing facilities for housing servers containing critical Aadhaar related information. AUA/KUA should deploy label, monitor and test regularly the operation of fire exit doors and fire extinguishing systems.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8		
61.	Preventive maintenance activity at data centre	AUA/KUA should ensure that preventive maintenance activities, such as audit of fire extinguishers and CCTV, are carried out on a quarterly basis.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8		
62.	Physical location of AUA/KUA servers	AUA/KUAshould ensure thatthe data centres hosting servers on which	• The Aadhaar (Authenticati on and Offline		

J.	Data security	Aadhaar related information is stored are within India.	•	Verification) Regulations, 2021 — Chapter III — sub- regulation (1) of regulation 22 UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9		
63.	PID encryption and biometric data security	AUA/KUA shouldensure that biometric data are necessarily encrypted and secured at the time of capture of such information of the Aadhaar number holder,in accordance with such specifications as UIDAI may lay down from time to time.	•	(Authenticati on and Offline Verification) Regulations, 2021 — Chapter II — Sub- regulation (2) of regulation 7		
64.	PID encryption and biometric data security	AUA/KUA should ensure that after collection of requisite demographic	•	The Aadhaar (Authenticati on and Offline		

		1,	1	TT 10	Γ	Γ	
		and/or biometric information and/or one-time password (OTP) from the Aadhaar number holder, the client application immediately packages and encrypts these input parameters into a PID block, before transmitting the same, and that the same is sent to the server of the AUA/KUA using secure protocols.	•	Verification) Regulations, 2021 — Chapter II — Sub- regulation (1) of regulation 9 The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter II — Sub- regulation (5) of regulation 9 UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section			
65.	PID encryption and biometric	AUA/KUA should ensure that the PID	•	2.7 UIDAI Aadhaar			
	data security	block is encrypted with a dynamic session key using AES 256 symmetric algorithm (AES/GCM/No Padding) at the time of capture on the authentication device. The session key should be encrypted with 2048-bit UIDAI	•	Authenticatio n Application Security Standard UIDAI Aadhaar Authenticatio n API Specification Version 2.5			

66.	PID encryption and biometric data security	public key using asymmetric algorithm (RSA/ECB/PKCS1 Padding). In doing so, AUA/KUA should comply with the latest API specification document issued by UIDAIfrom time to time. AUA/KUA should ensure with respect to the operational details referred to	• UIDAI Aadhaar Authenticatio n		
		against control number 65, that the session key is not stored anywhere except in the memory and that the same is not reused across transactions. Reuse of session key is allowed only when it is used as seed key while using synchronised session key scheme.	 Application Security Standard UIDAI Aadhaar Authenticatio n API Specification Version 2.5 		
67.	Aadhaar number security	AUA/KUA should ensure that the Aadhaar number/ Virtual ID (VID) /ANCS token provided by the Aadhaar number holder for authentication request is not retained by the device operator or within the device or at the AUA/KUA	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (ca) of sub- regulation (1) of regulation 14		

		server(s).			
68.	Restriction in	AUA/KUA should	The Aadhaar		
	storage of	ensure that under	(Authentication		
	Aadhaar	no circumstances	and Offline		
	number,	assisted devices	Verification)		
	biometrics	and any application	Regulations,		
	and/or eKYC of	associated with	2021 — Chapter		
	Aadhaar number	Aadhaar	III — Clause (a)		
	holder	authentication	of sub-		
		stores the Aadhaar	regulation (1) of		
		number, biometrics	regulation 17		
		and/or e-KYC of			
		the Aadhaar			
		number holder.			
69.	Fingerprint	For fingerprint-	UIDAI circular		
	biometric data	based biometric	Κ		
	(FMR and FIR)	authentication	11022/198/2017		
	capture in single	devices,	-UIDAI (Auth-		
	PID block	AUA/KUA should	I), dated		
		ensure capture of	11.11.2021		
		Finger Minutiae			
		Record (FMR) and			
		Finger Image Record (FIR) in			
		single PID block.			
70.	Security of	AUA/KUA should	Aadhaar		
70.	private keys	ensure that the	Authentication		
		private key used	API		
		for digitally signing			
		the authentication	Version 2.5		
		request and the			
		licence keys are			
		kept secure and the			
		access to the same			
		is controlled, and			
		that the private key			
		meetssuch			
		parametersas			
		UIDAImay specify			
		from time to time			
		in the Aadhaar			
		Authentication API			
		Specification			

		document issued by			
		it.			
		11.			
71.	Use of HSM	AUA/KUA should	UIDAI circular		
, 1.		ensure that key(s)	K		
		• • • •	K 11020/204/2017		
		used for digitally			
		signing	-UIDAI (Auth-		
		authentication	I), dated		
		requests and	22.6.2017		
		decrypting e-KYC	(Implementation		
		XML responses are	of HSM by		
		stored only in the	Entity/ASA)		
		Hardware Security			
		Module (HSM),			
		which should be			
		compliant with the			
		latest FIPS 140-2			
		standard.			
		AUA/KUA should			
		comply with all the			
		requirements of			
		UIDAI circular no.			
		K 11020/204/2017-			
		UIDAI (Auth-I), dated 22.6.2017			
		(Implementation of			
		HSM by			
		Entity/ASA).			
72.	Use of HSM	AUA/KUA should	UIDAI		
		have a dedicated,	Information		
		on-premise, HSM	Security Policy		
		setup for the	— UIDAI		
		management of	External		
		security/encryption	Ecosystem —		
		keys, and should	Section 2.7(7)		
		not share the same			
		with any other			
		entity.			
73.	Use of ADV	An AUA/KUAand	UIDAI circular		
		any other entity	K-		
		which is allowed to	11020/205/2017		
		store Aadhaar	-UIDAI (Auth-		
		number should	I), dated		
		collect and store	25.7.2017		
		confect and store	23.1.2017		

		Aadhaar number	(Circular for		
			Aadhaar Data		
		and any connected			
		data only in a	Vault)		
		separate, secure			
		database/vault/syst			
		em, termed as			
		Aadhaar Data			
		Vault (ADV).			
		Such AUA/KUA			
		should ensure that			
		each Aadhaar			
		number is referred			
		to by an additional			
		key, called as			
		reference key, and			
		that mapping of the			
		reference key and			
		Aadhaar number is			
		maintained in			
		ADV.			
74.	Use of Aadhaar	AUA/KUA should	UIDAI		
	data vault	ensure that if ADV	Guidelines for		
	(ADV) on cloud	is hosted on cloud,	ADV on Cloud		
		the ADV cloud			
		service complies			
		with UIDAI's			
		Guidelines for			
		ADV on Cloud.			
		The ADV should			
		be hosted only by			
		Government			
		Community Cloud			
		(GCC) service			
		providers,			
		recognised as such			
		by the Ministry of			
		Electronics and			
		Information			
		Technology.			
75.	Use of ADV on	AUA/KUA having	UIDAI		
15.	cloud	ADV on cloud	Guidelines for		
	cioud				
		should get annual	ADV on cloud		
		SOC2 Type II			
		examination			
		performed for			
		cloud hosting			

		•			
		service.			
		Management			
		review should be			
		performed for non-			
		compliant /			
		qualified controls			
		reported in the			
		SOC2 Type II			
		reports.			
76.	Use of ADV	AUA/KUA should	UIDAI circular		
		ensure that	no. K-		
		Aadhaar numbers	11020/205/2017		
		along with	-UIDAI (Auth-		
		connected data	I), dated		
		(such as eKYC	25.7.2017		
		XML containing	(Circular for		
		Aadhaar numbers	Aadhaar Data		
		and demographic	Vault)		
		data), if any, is			
		stored only in a			
		single logical			
		instance of ADV,			
		along with			
		corresponding			
		reference key.			
		AUA/KUA should			
		ensure that			
		appropriate High			
		Availability and			
		Disaster Recovery			
		provisions are			
		made for the vault,			
		with the same level			
		of security.			
77.	Use of ADV	AUA/KUA should	UIDAI circular		
,,,.		ensure that only	no. K-		
		trusted	11020/205/2017		
		communications	-UIDAI (Auth-		
		are permitted in	I), dated		
		and out of the	25.7.2017		
		vault; this should	(Circular for		
		ideally be done	Aadhaar Data		
		through	Vault)		
		APIs/microservices			
		dedicated to obtain			
		the mapping and			
		controlling the			

	access to the APIs/microservices at the application level.			
	AUA/KUA should ensure that any authorised users needing to access such mapping necessarily go through the application for viewing/accessing the data, after appropriate user			
	authentication, authorisation and logging.			
78. Use of A		UIDAI circular K- 11020/205/2017 -UIDAI (Auth- I), dated 25.7.2017 (Circular for Aadhaar Data Vault)		
79. End-poi security	-	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4		
80. End-poin security antivirus malware	use licensed/ anti-malware and	UIDAI Information Security Policy — UIDAI		

		(proforably Nant	Extornal		
		(preferably Next-	External		
		Generation	Ecosystem —		
		antivirus) to protect	AUA KUA —		
		against malware.	Section 2.9(10)		
		The			
		malware/antivirus			
		installed should be			
		configured to			
		update in real time.			
81.	Aadhaar	AUA/KUAshould	The Aadhaar		
01.	information	mask Aadhaar	(Authentication		
			•		
	security —	numbers collected	and Offline		
	Physical	through physical	Verification)		
	Aadhaar	forms or	Regulations,		
	documents	photocopies of	2021 — Chapter		
		Aadhaar letters, by	III — Clause		
		masking the first	(mb) of sub-		
		eight digits of the	regulation (1) of		
		Aadhaar number,	regulation (14)		
		before storing			
		physical copies.			
82.	Use of security	AUA/KUA and	UIDAI		
02.	communication	ASA should ensure	Information		
	protocols	message security	Security Policy		
		and integrity	— UIDAI		
		between their	External		
		servers and those	Ecosystem —		
		of third party	Section 2.11(6)		
		entities, such as			
		Sub-AUAs and			
		Sub-KUAs.			
		AUA/KUA should			
		procure digital			
		certificate from a			
		Certifying			
		Authority as			
		defined in the IT			
		Act.			
83.	Restriction on	AUA/KUA, Sub-	UIDAI		
	display/	AUAs, Sub-KUAs,	Information		
	publishing of	Business	Security		
	identity	Correspondents	Policy—UIDAI		
	information	and other sub-	External		
		contractors	Ecosystem —		
		performing	AUA KUA —		
		Aadhaar	Section 2.9		

		authentication should ensure that identity information is not displayed or disclosed to external agencies or unauthorised persons.			
84.	Restriction in display/ publishing of identity information	AUA/KUA should not publish any personal identifiable data including Aadhaar in public domain/websites etc.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.9		
85.	Restriction in display/ publishing of identity information	AUA/KUA should ensure that display of full Aadhaar number is controlled only for the Aadhaar number holder or for such special roles/users of AUA/KUA as havefunctional necessity for the same; by default, all other display should be masked such that only the last four digits of the Aadhaar number are displayed.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.7(10)		
86.	End-point security	AUA/KUA should ensure that end- point devices used for developing, process and handling Aadhaar data and application timeout after a session is idle for more than	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(29)		

		20 to 15 minutes				
		30 to 15 minutes,	• UIDAI			
		based on the	Information			
		criticality of the	Security			
		application.	Policy —			
			UIDAI			
			External			
			Ecosystem —			
			AUA KUA			
			— Section			
			2.9(30)			
87.	Secure software	AUA/KUA should	UIDAI			
07.			Information			
	development	implement system				
		and processes to	Security Policy			
		ensure secure	— UIDAI			
		software	External			
		development	Ecosystem —			
		practices.	Section 2.9(5)			
		Periodic training of				
		developers should				
		be conducted on				
		secure software				
		development				
		practices. Records				
		of such trainings				
		should be				
		maintained.				
88.	Restriction in	AUA/KUA should	• UIDAI			
	local storage of	ensure that there is	Information			
	Aadhaar data /	no local storage of	Security			
	PII information	Aadhaar number or	Policy —			
		VID or the PID	UIDAI			
		block on the	External			
		system, volatile	Ecosystem			
		memory or the	— Section			
		database.	2.9(19)			
			• UIDAI			
		Incase of a mobile	circular no/			
		application,				
		AUA/KUA should	K-			
			11020/217/2			
		ensure that there is	018-UIDAI			
		no local storage of	(Auth-I),			
		Aadhaar number or	dated			
		the PID block in	1.5.2018			
		the shared	(Implementat			
		preference folder.	ion of Virtual			
			ID, UID			
		1	,	l	l	I

89. Encryption of stored eKYC AUA/KUA should UIDAI stored eKYC Information	
KYC) 89. Encryption of AUA/KUA should UIDAI	
89. Encryption of AUA/KUA should UIDAI	
stored eKYC ensure that e-KYC Information	
data data is stored in an Security Policy	
encrypted manner — UIDAI	
in database tables. External	
Ecosystem —	
Section 2.9(18)	
90. Patch AUA/KUA should UIDAI	
management ensure that the Information	
patch management Security Policy	
process is — UIDAI	
implemented for External	
applying patches to Ecosystem —	
information AUA KUA —	
systems. Patches Section 2.9(8)	
should be updated	
at both the	
application and the	
server and network	
levels.	
AUA/KUA should	
ensure that either N	
or N-1 patches are	
maintained.	
K. Network security	
91. Network AUA/KUA should • The Aadhaar	
connectivity establish secure (Authenticati	
with ASA network on and	
connectivityOfflinebetweenVerification)	
Sub-AUAs, Sub- 2021 —	
KUAs, sub- Chapter III	
contractors and — Clause (c)	
ASAs, and should of sub-	
connect with ASAs regulation	
only through secure (1) of	
leased lines or regulation 14	
similar secure • UIDAI	
private lines. If a Information	
public network is Security	
used, only a secure Policy —	
channel should be UIDAI	

		used	Extomol		
		used.	External		
			Ecosystem		
			—Sections		
			2.9 and 2.11		
92.	Segregation of	AUA/KUAshoulde	UIDAI		
	AUA	nsure that its	Information		
	serversnetwork	servers reside in a	Security		
		segregated network	Policy—UIDAI		
		segment isolated	External		
		from the rest of the	Ecosystem —		
		network of the	AUA KUA —		
		AUA/KUA	Section 2.9		
		organisation. The			
		AUA/KUA			
		serversshould be			
		dedicated for			
		online Aadhaar			
		authentication			
		purposes and			
		should not be used			
		for any other			
		activities not			
		related to Aadhaar.			
93.	Firewall access	AUA/KUA should	UIDAI		
	of network	ensure that	Information		
		authentication	Security Policy		
		application servers	— UIDAI		
		and infrastructure	External		
		are hosted behind a	Ecosystem —		
		firewall and that	AUA KUA —		
		firewall rules block	Section 2.11 (4)		
		incoming access			
		requests to the			
		AUA/KUA server			
		from all sources			
		other than			
		whitelisted IP			
		addresses/zones.			
94.	NIPS/IDS	AUA/KUA should	UIDAI		
	implementation	ensure that network	Information		
	1	intrusion and	Security Policy		
		prevention systems	— UIDAI		
		(NIPS) and	External		
		intrusion detection	Ecosystem —		
		system (IDS) are	AUA KUA —		
		implemented to	Section 2.9 (11)		
		-	Section 2.9 (11)		
		safeguard the			

95.	Network security	network from external attacks / DDoS attacks. AUA/KUA should ensure that Internet access on systems are restricted to necessary or work- related websites and that access to web portals known	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4		
		for pirated software, gambling etc. are restricted.			
96.	Encryption of data on network	AUA/KUA should ensure that transmission of Aadhaar number across open, public networks is always encrypted,using the latest version of Transport Layer Security (TLS)configuration	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(7)		
L.	Operations secu	rity	1	1	
97.	Segregation of testing and production environments	AUA/KUA should ensure that the testing and production facilities/environm ents are physically and/or logically separated.	UIDAI Information Security Policy - UIDAI External Ecosystem — AUA KUA — Section 2.9		
		AUA/KUA should ensure that authentication application testing utilises test data / non-production data and thatAadhaar number holder's identity data are			

		not used for testing the application.			
98.	Restrictions on designing/ compiling malicious code	AUA/KUA personnel should not intentionally write, generate, compile, copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any Aadhaar information.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9		
99.	License key / encryption keys security	AUA/KUA should ensure that license keys are kept secure and access controlled, and that separate license keys are generated for their Sub-AUAs and Sub-KUAs from UIDAI's portal and kept secure and access to the same kept controlled.	 The Aadhaar (Authentica tion and Offline Verification) Regulations , 2021 — Chapter III — Sub- regulation (2) of regulation 15 The Aadhaar (Authentica tion and Offline Verification) Regulations , 2021 — Chapter III — Clause (f) of sub- 		

			1	[l
			regulation		
			(1) of		
			regulation		
			17		
			Information		
			Security		
			Policy—		
			UIDAI		
			External		
			Ecosystem		
			— AUA		
			KUA —		
			Section 2.9		
100.	Implementation	AUA/KUA must	UIDAI circular		
	of Virtual ID	provide in their	no. K-		
		authentication	11020/217/2018		
			-UIDAI (Auth-		
		application the			
		option for an	I), dated		
		Aadhaar number	1.5.2018		
		holder to use a	(Implementation		
		Virtual ID (VID)	of VID, UID		
		for authentication,	Token and		
		in place of their	Limited KYC)		
		Aadhaar number.			
101					
101.	UID Token	AUA/KUA should	UIDAI circular		
		make provision to	K-		
		store UID tokens in	11020/217/2018		
		their database.	-UIDAI (Auth-		
			I), dated		
			1.5.2018		
			(Implementation		
			-		
			of Virtual ID,		
			UID Token and		
			Limited KYC)	 	
102.	Restriction on	AUA/KUA should	UIDAI	 	
	the use of	ensure that	Information		
	Aadhaar as	Aadhaar	Security		
	domain-specific	numberand VIDare	Policy—UIDAI		
			-		
	identifier	never used as	External		
		domain-specific	Ecosystem —		
		identifiers and that	AUA KUA —		
		domain-specific	Section 2.9		
		identifiers are			
		revoked and/or			
		reissued. For			
1					
		example, instead of			

		using Aadhaar number as bank customer ID or license number or student ID etc., a local, domain- specific identifier mapped in the back-end database should be used.			
103.	Unique device code of each device	AUA/KUA should ensure that each authentication device has a unique device code and that a unique transaction number is automatically generated by the authentication device and incremented for each transaction processed.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.11 (1)		
104.	Back-up / alternative identity authentication mechanism	AUA/KUA should implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to Aadhaar number holders.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (i) of sub- regulation (1) of regulation 14		
105.	Notification to Aadhaar number holders	AUA/KUA should notify the Aadhaar number holder of the success or failure of each authentication request, through email and/or SMS. Such notification should shall	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — sub- regulations (1), (2) and (3) of regulation 10		

		1 1 1 2			I
		include the name of			
		the requesting			
		entity, the date and			
		time of			
		authentication, the			
		authentication			
		response code (in			
		case of online			
		authentication), the			
		last four digits of			
		the Aadhaar			
		number and the			
		purpose of			
		authentication, as			
		the case may be.			
		5			
		In case of			
		authentication			
		failure, the			
		AUA/KUA should,			
		in clear and precise			
		language, inform			
		the Aadhaar			
		number holderof			
		the reasons of			
		authentication			
		failure, such as			
		"Aadhaar			
		cancelled",			
		"Aadhaar			
		deactivated",			
		"Aadhaar locked",			
		"Aadhaar omitted",			
		"Aadhaar			
		suspended" and			
		"Biometrics			
		locked".			
106.	Establishment of	AUA/KUA should	Authentication		
100.	grievance	have an effective	User Agency		
	handling	grievance handling	Agreement		
	mechanism	mechanism and	version 6.0 —		
	meenamism	provide the same	Paragraph 14.3		
		through multiple	1 aragraph 14.5		
		channels.			
		channels.			

107	Crience		A with a method of]
107.	Grievance	AUA/KUAshould	Authentication		
	handling	ensure that its Sub-	User Agency		
	mechanism of	AUAs and Sub-	Agreement		
	Sub-AUAs and	KUAs have a	version 6.0 —		
	Sub-KUAs	grievance handling	Paragraph 14.3		
		mechanism to			
		receive and address			
		complaints from			
		Aadhaar number			
		holders regarding			
		authentication			
		facilities performed			
		by them.			
108.	Aadhaar	Whereapplicable,	UIDAI Circular		
	authentication	AUA/KUA should	Notification		
	for banks	comply with	No.		
		notification no.	13012/79/2017/		
		13012/79/2017/Leg	Legal-UIDAI		
		al-UIDAI (No. 6 of	(No. 6 of 2017),		
		2017), dated	dated		
		19.12.2017,	19.12.2017		
		regarding the	17.12.2017		
		process for placing			
		and overriding bank accounts on			
		Aadhaar Payments			
		Bridge (APB) —			
		National Payments			
		Corporation of			
		India (NPCI)			
		Mapper. In			
		particular, the			
		AUA/KUA should			
		comply with the			
		following:			
		(a) Override			
		request			
		pertaining			
		to an			
		Aadhaar			
		number			
		holder			
		should be			
		accompanie			
		d by the			
		name of			
		his/her			

		T
	current	
	bank on the	
	APB	
	mapper and	
	confirmatio	
	n from the	
	requesting	
	bank that it	
	has	
	obtained the	
	requisite	
	consent of	
	the Aadhaar	
	holder for	
	switching to	
	the	
	requesting	
	bank on the	
	mapper.	
	(b) Send	
	request for	
	mapping of	
	a new	
	account or	
	overriding	
	an existing	
	bank	
	account to	
	NPCI only	
	after taking	
	explicit,	
	informed	
	consent of	
	the	
	customer.	
	(c) Inform each	
	accounthold	
	er through	
	SMS and	
	email,	
	within 24	
	hours, that a	
	request has	
	been sent to	
	NPCI to put	
	his/her bank	
	account on	
· · · · · · · · · · · · · · · · · · ·		

the mapper	
or, as the	
case may	
be, to	
change his	
bank	
account on	
the NPCI	
mapper	
(while	
providing	
the name of	
current	
bank on the	
mapper and	
the last four	
digits of the	
account	
number of	
the new	
bank, along	
with the	
bank name)	
and, in case	
he/she does	
not want to	
put his/her	
new bank	
account on	
the mapper,	
provide the	
customer an	
option to	
reverse	
such	
mapping.	
(d) If an	
accounthold	
er does not	
have an	
email or	
mobile	
number and	
communicat	
ion cannot	
be sent,	
his/her	

physical	
signature on	
a paper	
consent	
form should	
be obtained	
prior to	
sending the	
request to	
the NPCI	
mapper.	
(e) The records	
of consents	
obtained in	
(b) and the	
communicat	
ions made	
in items (a),	
(b) and(c)	
and scanned	
copy of the	
consent	
form in (d)	
should be	
retained for	
seven years	
by the bank,	
in	
accordance	
withthe	
Aadhaar	
(Authentica	
tion and	
Offline	
Verification	
)	
Regulations	
, 2021.	
(f) Make	
available	
the	
aforesaid	
records at	
the time of	
audit, in	
accordance	
with the	
with the	

M.	Application secu	Aadhaar (Authentica tion and Offline Verification) Regulations , 2021. rity		
109.	Compliance to API specifications and application security	AUA/KUA should ensure that the client applications and software used for authentication should conform to the latest API standards and specifications laid down by UIDAI from time to time, and that itsSub- AUAs and Sub- KUAs use client applications or software development kit (SDK) developed or digitally signed by the AUA/KUA.	 The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter II — Sub- regulation (2) of regulation 8 and Chapter III — Clause (a) of sub- regulation (3) of regulation 15 UIDAI Aadhaar Authenticatio n Application Security Standard, version 1.0, 2020 UIDAI Aadhaar Authenticatio n Application Security Standard, version 1.0, 2020 UIDAI Aadhaar Authenticatio n API Specification Version 2.5, Revision 1, January 2022 	

and AP1 ensure that it has Information gateway AP1 whitelist Sconity Policy implementation Limit the data External exchange using Ecosystem — Ouly authorised AP1 whitelist Scolity Policy Ecosystem — ouly authorised APIs and with Scolity 2.10(4) APIs and with Scolity 2.10(4) Scolity 2.10(4) addresses AUA/KUA should also ensure that API gateway is deployed for Centralised security enforcement, monitoring and management. AUA/KUA should ensure that rate Iminition and Iminition and Distributed Denial Scolity 2.10(4) Distributed Denial Scolity 2.10(4) Scolity 2.10(4) Bistributed Denial Scolity 2.10(4) Scolity 2.10(4) Of Service (DDOS) attacks. Scolity 2.10(4) Distributed Denial Scolity 2.10(4) Scolity 2.10(4) Bistributed Denial Scolity 2.10(4) Scolity 2.10(4) Distributed Denial Scolity 2.10(4) Scolity 2.10(4) Distributed Denial Scolity 2.10(4		1	1		1	1	1
gateway implementation API whitelist implemented to implemented to exchange using only authorised APIs and with whitelisted IP addresses. Section 2.10(4) Image: Construction of the construct	110.	API whitelisting	AUA/KUA should	UIDAI			
implementation implemented to UIDA1 imit the data External exchange using Ecosystem only authorised Section 2.10(4) APIs and with whitelisted 1P addresses. AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement. monitoring and management. AUA/KUA should ensure that rate imitation and imitation and management. AUA/KUA should ensure that rate imitation and management. AUA/KUA should ensure that rate imitation and management. AUA/KUA should ensure that rate imitation and monitoring and management. AUA/KUA should of Service (DDoS) attacks. attacks. AUA/KUA should ensure that Cross- Origin Resource Origin Resource Sharing (CORS) parameters are configured to restrict mantorised domains from accessing APIs		and API	ensure that it has	Information			
111. Source code AUA/KUA should 211. Source code AUA/KUA should <td< th=""><th></th><th>gateway</th><th>API whitelist</th><th>Security Policy</th><th></th><th></th><th></th></td<>		gateway	API whitelist	Security Policy			
11. Source code AUA/KUA should 21.01 AUA/KUA should 22.01 AUA/KUA should 23.01 AUA/KUA should 24.01 AUA/KUA should 25.01 AUA/KUA s		implementation	implemented to	— UIDAI			
11. Source code AUX/KUA should 211. Source code AUX/KUA should		_	limit the data	External			
11. Source code AUX/KUA should 211. Source code AUX/KUA should			exchange using	Ecosystem —			
11. Source code AUA/KUA should also ensure that AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and through the state of the				=			
11. Source code AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management. Image: monitor in gateway is deployed for centralised security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and throuting mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks. Image: monitor in gateway is deployed for centralises accurate that a coss-Origin Resource Sharing (ORS) shar							
11. Source code AUA/KUA should also ensure that API gateway is addresses. AVAPI gateway is deployed for entraited security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and through the methanism are implemented to prevent abuse of API and Distributed Denial of Service (DDoS) attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict insuthorised domains from accessing APIs ensure that Cross- from the client side. utDAI utDAI							
11. Source code AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDoS) attacks. AUA/KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. AUA/KUA should UIDAI 111. Source code AUA/KUA should UIDAI UIDAI							
111. Source code AUA/KUA should Image: Constrained security Image: Constrained security Image: Constrained security </th <th></th> <th></th> <th>auuresses.</th> <th></th> <th></th> <th></th> <th></th>			auuresses.				
111. Source code AUA/KUA should Image: Constrained security Image: Constrained security Image: Constrained security </th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
11. Source code AUA/KUA should Image: Construction of the structure of the struct							
111. Source code AUA/KUA should Image: Source or Source of Source or So							
111. Source code AUA/KUA should anagement. AUA/KUA should ensure that rate imitation and imitation and throttling mechanisms are implemented to prevent abuse of API and AVI/KUA should ensure that rate implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client isde 111. Source code AUA/KUA should							
111. Source code AUA/KUA should enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks. Image: Comparison of the second of Service (DDOS) attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. Image: Comparison of the second of the							
111. Source code AUA/KUA should anaagement. AUA/KUA should anaagement. AUA/KUA should anaagement. auaagement. AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks. attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side.							
111. Source code AUA/KUA should anagement. AUA/KUA should ensure that rate imitation and imitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. UIDAI							
111. Source code AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks. 111. Source code AUA/KUA should ensure that Cross-from the client side. 111. Source code AUA/KUA should UIDAI			monitoring and				
111. Source code AUA/KUA should UIDAI Image: Construction of the client side. 111. Source code AUA/KUA should Image: Construction of the client side. Image: Construction of the client side. Image: Construction of the client side. 111. Source code AUA/KUA should Image: Construction of the client side. 111. Source code AUA/KUA should Image: Construction of the client side. Image: Construction of the client			management.				
111. Source code AUA/KUA should UIDAI Image: Construction of the client side. 111. Source code AUA/KUA should Image: Construction of the client side. Image: Construction of the client side. Image: Construction of the client side. 111. Source code AUA/KUA should Image: Construction of the client side. 111. Source code AUA/KUA should Image: Construction of the client side. Image: Construction of the client							
111. Source code AU/KUA should IIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			AUA/KUA should				
111.Source codeAUA/KUA shouldImage: Code code code code code code code code c			ensure that rate				
Image: Source codemechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDOS) attacks.Image: Source (DDOS) attacks.AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side.Image: Source of the source of the source to the source of the source o			limitation and				
111. Source code AUA/KUA should Image: Source			throttling				
111. Source code AU/KUA should Image: Code of the			mechanisms are				
111. Source code AU/KUA should Image: Code of the			implemented to				
API and Distributed Denial of Service (DDoS) attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. 111. Source code AUA/KUA should							
Distributed Denial of Service (DDoS) attacks. Image: Comparison of Service (DDoS) attacks. Image: Comparison of Service (DDoS) attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) Image: Comparison of Service (DDoS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. Image: Comparison of Service (DDoS) 111. Source code AUA/KUA should UIDAI Image: Comparison of Service (DDoS)			-				
111. Source code AUA/KUA should attacks. AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict Configured to restrict unauthorised domains from accessing APIs from the client side. Image: Configured to 111. Source code AUA/KUA should							
111.attacks.AUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side.111.Source codeAUA/KUA should UIDAI							
111.Source codeAUA/KUA should ensure that Cross- Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side.Image: Comparison of the client side.Image: Comparison of the client side.Image: Comparison of the client side.111.Source codeAUA/KUA shouldUIDAIImage: Comparison of the client side.Image: Comparison of the client side.							
111.Source codeAUA/KUA shouldUIDAIII <tdi< td=""><td></td><td></td><td>attacks.</td><td></td><td></td><td></td><td></td></tdi<>			attacks.				
111.Source codeAUA/KUA shouldUIDAIII <tdi< th=""><th></th><th></th><th>AUA/KUA should</th><th></th><th></th><th></th><th></th></tdi<>			AUA/KUA should				
111.Source codeAUA/KUA shouldUIDAIImage: Constant of the c							
111.Sharing (CORS)parameters are configured to restrict unauthorised domains from accessing APIs from the client side.111.Source codeAUA/KUA shouldUIDAIImage: Construct Image: Construct<							
111.parameters are parameters are configured to restrict unauthorised domains from accessing APIs side.Image: Configured to restrict to the client side.Image: Configured to to the client to the client to the clientImage: Configured to to the clientImage: Configured to to the client to the clientImage: Configured to to the clientImage: Configured to to the clientImage: Configured to to the client111.Source codeAUA/KUA shouldUIDAIImage: Configured to to the clientImage: Configured to to the clientImage: Configured to to the client			-				
111.configured to restrict unauthorised domains from side.lane lane lane lane lanelane lane lane lane lanelane lane lane lane lane lane lane lanelane lane lane lane lane lane lane lanelane lane lane lane lane lane lane lanelane lane lane lane lane lanelane lane lane lane lanelane lane lane lane lanelane lane lane lanelane lane lane lanelane lane lane lanelane lane lanelane lane lanelane lane lane lanelane lane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lanelane lane lane lanelane lane lane lanelane lane lane lane lanelane <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
restrictrestrictunauthorisedunauthoriseddomains fromdomains fromaccessing APIsfrom the clientfrom the clientside.in the client111.Source codeAUA/KUA shouldUIDAIin the client							
unauthorised unauthorised domains from accessing APIs from the client ide. 111. Source code AUA/KUA should UIDAI							
domains from accessing APIs from the client from the client side. Image: Control of the client 111. Source code AUA/KUA should UIDAI							
accessing APIs accessing APIs from the client from the client side. accessing APIs 111. Source code AUA/KUA should UIDAI							
from the client from the client side. Image: Control of the client 111. Source code AUA/KUA should UIDAI							
side. side. 111. Source code AUA/KUA should UIDAI							
111. Source code AUA/KUA should UIDAI			from the client				
			side.				
	111.	Source code	AUA/KUA should	UIDAI			
review by perform source Information		review by	perform source	Information			
CERT-In- code review of the Security Policy		-		Security Policy			

	empanelled	modules and	— UIDAI		
	auditor	applications used	External		
		for authentication	Ecosystem —		
		and e-KYC and	Section 2.10(5)		
		undergo audit by a			
		CERT-In-			
		empanelled auditor.			
112.	SAST/DAST	AUA/KUA should	UIDAI		
	application audit	ensure that	Information		
	apprivation addit	authentication	Security Policy		
		application security	— UIDAI		
		assessment	External		
		{including static	Ecosystem —		
		application security	Section 2.10(6)		
		testing (SAST) and	5000000 2.10(0)		
		dynamic			
		application security			
		testing (DAST)} is			
		performed at least			
		annually or at the			
		time of major			
		changes to the			
		authentication			
		application, and that all			
		vulnerabilities are			
		addressed for			
		remediation and no			
		vulnerable third			
		party components			
		are used by the			
		authentication			
110	X71 1 '1'	application.			
113.	Vulnerability	AUA/KUA should	UIDAI		
	assessment	plan organisation	Information		
		information	Security Policy		
		security policy,	— UIDAI		
		inclusive of	External		
		vulnerability	Ecosystem —		
		assessment and	Section 2.10(6)		
		penetration testing			
		on its network,			
		infrastructure and			
		applications.			
114.	Configuration	AUA/KUA should	UIDAI		
	reviews and	ensure that	Information		
	system	authentication	Security Policy		

	walkthrough	applications are	— UIDAI
	warktinough	integrated with	External
		IDAM, PIM/PAM	Ecosystem —
		and SIEM.	Section 2.11(8)
115.	Application	AUA/KUA should	UIDAI
115.	Application		
	code review	ensure that the	Information
		passwords, tokens,	Security Policy
		security keys and	
		licenses are not	External
		hardcoded in the	Ecosystem —
		application code.	Section 2.10(5)
N.	Logging and mo		
116.	Authentication	AUA/KUA should	• The Aadhaar
	log maintenance	maintain logs of	(Authenticati
		the authentication	on and
		transactions	Offline
		processed by it,	Verification)
		which should	Regulations,
		contain the	2021 —
		following	Chapter III
		transaction details:	— Sub-
		(a) specified	regulation
		parameters	(1) of
		of	regulation 18
		authenticati	• UIDAI
		on request	Information
		submitted;	Security
		(b) specified	Policy —
		parameters	UIDAI
		received as	External
		authenticati	Ecosystem
		on	— AUA
		response;	KUA —
		(c) the record	Section 2.9
		of	(15)
		disclosure	• UIDAI
		of	Information
		information	Security
		to the	Policy —
		Aadhaar	UIDAI
		number	External
		holder at	
		the time of	Ecosystem
		authenticati	— AUA
		on; and	KUA —
			Section 2.9
		(d) record of	(16)
		consent of	

		.			۱ ۱
		the Aadhaar			
		number			
		holder for			
		authenticati			
		on, but shall			
		not, in any			
		event, retain			
		the PID			
		information			
		, Aadhaar			
		number/			
		VID.			
117.	Authentication	AUA/KUA should	The Aadhaar		
11/1	log retention	ensure that the logs	(Authentication		
	log recention	of authentication	and Offline		
		transactions are	Verification)		
		stored online for	Regulations,		
			2021 — Chapter		
		audit purposes for	III — sub-		
		two years and,			
		thereafter, archived	regulations (2) and (2) of		
		for another five	and (3) of		
110		years.	regulation 18		
118.	Retention of	AUA/KUA should	The Aadhaar		
	transaction logs	maintain auditable	(Authentication		
	of Sub-	logs of all such	and Offline		
	AUA/Sub-KUA	transactions where	Verification)		
		e-KYC data has	Regulations,		
		been shared with	2021 — Chapter		
		any of its Sub-	III — Sub-		
		AUAsand Sub-	regulation (6) of		
		KUAs, for such	regulation 16		
		period as UIDAI			
		may specify from			
		time to time.			
119.	Security	AUA/KUA should	UIDAI		
	incident	ensure that the	Information		
	recording	event/security logs	Security Policy		
		recording critical	— UIDAI		
		user-activities,	External		
		exceptions and	Ecosystem —		
		security events are	AUA KUA —		
		enabled and stored	Section 2.9(12)		
		to assist any future			
		investigation and			
		enable access			
		control monitoring.			
l		control monitoring.			

120.	Security incident monitoring	AUA/KUA should ensure that regular monitoring of event/security logs takes place to detect unauthorised use of information systems and that results of the same are recorded. Further, access to audit trails and event logs should be provided to	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(13)		
121.	Clock	authorised personnel only. AUA/KUA should	• UIDAI		
	synchronisation through use of Network Time Protocol (NTP)	ACA/KCA should connect to the Network Time Protocol (NTP) server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to the said NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC; however, it should be ensured that such time source does not deviate from NPL and NIC.	 OIDAT Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9 (22) CERT-In Directive No. 20(3)/2022- CERT-In dated 28.4.2022 		

0.	Fraud and foren	isics				
122.	Fraud analytics	AUA/KUAshould	UIDAI			
	module	deploy, as part of	Information			
		its systems, a fraud	Security Policy			
		analytics module	— UIDAI			
		that is capable of	External			
		analysing	Ecosystem —			
		authentication	AUA KUA —			
		related transactions	Section 2.13 (9)			
		to identify fraud.				
Р.	Providing Aadh	aar Authentication fa	cilities to Sub-AU	As and Sub-KUA	S	
123.	Approval from	AUA/KUA should	UIDAI			
	UIDAI for	obtain approval	Information			
	appointment of	from UIDAI before	Security			
	Sub-AUA/Sub-	appointing any	Policy—UIDAI			
	KUA	entity as its Sub-	External			
		AUA or Sub-KUA,	Ecosystem —			
		and should also	AUA KUA —			
		take permission in	Section 2.13			
		respect of anyentity				
		already appointed				
		as a Sub-AUA or				
		Sub-KUA.				
124.	Authentication	AUA/KUA should	UIDAI Circular			
	application	ensure that the	K11022/460/20			
	security	authentication	16-UIDAI			
		application to be	(Auth-II), dated			
		used or being used	28.2.2017 —			
		for Aadhaar	Clause 1(i)			
		authentication by				
		its Sub-AUAs and				
		Sub-KUAs is				
		developed and be				
		digitally signed by				
		AUA/KUA.				
125.	Authentication	AUA/KUA should	UIDAI Circular			
	application	ensure that the	K11022/460/20			
	security	authentication	16-UIDAI			
		application used by	(Auth-II), dated			
		its Sub-AUAs and	28.2.2017 —			
		Sub-KUAs does	Clause 1(ii)			
		not store biometric				
		data under any				
		circumstance, and that the biometrics				
		/ PID block is				

		an amount ad at the			
		encrypted at the			
		front-end device /			
		client level.			
126.	Authentication	AUA/KUA should	UIDAI Circular		
	application	ensure that the	no.		
	security	client	K11022/460/20		
		application(s) of its	16-UIDAI		
		Sub-AUAs and	(Auth-II) dated		
		Sub-KUAs does/do	28.2.2017 —		
		not, under any	Clause 1(iii)		
		circumstance,			
		replay the			
		authentication			
		request using			
		stored biometric			
		data.			
127.	Authentication	AUA/KUA should	UIDAI Circular		
	application audit	ensure that the	no.		
		authentication	K11022/460/20		
		application of its	16-UIDAI		
		Sub-AUAs and	(Auth-II), dated		
		Sub-KUAs are	28.2.2017 —		
		audited by the	Clause 1(iv)		
		Standardisation			
		Testing and Quality			
		Certification			
		(STQC)			
		Directorate of the			
		Ministry of			
		Electronics and			
		Information			
		Technology or a			
		CERT-In-			
		empanelled auditor			
		and a compliance			
		report is submitted to UIDAI.			
		AUA/KUA should			
		also ensure that all			
		its Sub-AUAs and			
		Sub-KUAs access			
		Aadhaar			
		Authentication			
		facilities only			
		through duly			
		audited			
		authentication			

applications.		